Module 4: Divisibility and Arithmetic

1. Determine $x \operatorname{div} y$ and $x \bmod y$ for each pair of values below.
   a. $x = 252, \quad y = 7$
   b. $x = 1398, \quad y = 13$
   c. $x = -21, \quad y = 33$
   d. $x = -457, \quad y = 22$

2. Determine the value for each of the following. These can be done without a calculator.
   a. 9×3 in $\mathbb{Z}_{20}$
   b. $15^{26} \bmod 7$
   c. $(352 \cdot 407) \bmod 50$
   d. $(1302^3 + 4505^2) \bmod 10$

Module 5: Prime Factorization, GCD, and Euclid's Algorithm

3. Determine if the following values are prime.
   a. 157
   b. 481
   c. 1907
   d. 2021

4 For each pair of x and y values below,

i) Determine the greatest common divisor (GCD) of x and y.

ii) Write the gcd(x, y) as a linear combination of x and y.

iii) Determine the multiplicative inverse of $x \bmod y$, if it exists.

---

a. $x = 45, \quad y = 55$

b. $x = 51, \quad y = 72$

c. $x = 39, \quad y = 44$

d. $x = 324, \quad y = 431$

Module 6: Number Representation in Other Bases

5 Convert each value below into decimal. The base is noted by the subscript.

a. $(523)_8$

b. $(2\text{B8E})_{16}$

c. $(101010)_2$

6 If the number is given in binary, convert it to hexadecimal. If the number is given in hexadecimal, convert it to binary.

a. $(7\text{E0})_{16}$

b. $(25\text{DAA})_{16}$

c. $(1100100101100000)_2$

d. $(11010011101111110101)_2$

7 Convert the following decimal values to the indicated base.

a. 716 in base 5

b. 500 in base 7

c. 1,000,000 in base 16

Module 7: Fast Exponentiation Algorithms

8. Answer the following questions about divisibility and modular arithmetic.
   a. What is the remainder of 3^{50} on division by 23?
   b. What is the remainder of 7^{117} on division by 11?
   c. Determine the value of $5^{44} \bmod 89$.

9. What are the last 4 bits in the binary representation of 3^{1402}

Module 8: Mathematical Foundations of Encryption

10. An encryption scheme converts letters to numbers in the following way: $A \to 07,\ B \to 08,\ \ldots$
$T \to 26,\ U \to 01,\ \ldots,\ Z \to 06$. Decrypt the message 102120262207201509.

11. Suppose that $p = 23$ and $q = 29$. Answer the following questions as they relate to the RSA encryption scheme described in this course.
   a. Determine the values of N and ϕ.
   b. Determine a valid value for e between 60 and 80. There is more than one possible value, so pick one for the next parts.
   c. With the value of e found in part b, determine the private key value d.
   d. Using the values found in the previous parts, encrypt the message $m =$ "15"

12. Answer the following questions about the RSA encryption system.
   a. Bobby chose the public key to be $N = 319$ and $e = 17$. Use this information to determine Bobby's private key, d.
   b. Determine which of the following are valid public keys. For those that are not valid, why not? If it is valid, find a possible private key.
      i $N = 49793, e = 12343$
      ii $N = 629, e = 421$
      iii $N = 6077, e = 987$