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. $x = -457, \quad y = 22$

Solution: Using the Division Algorithm in Lesson 2.3:

a. $252 = 36 \cdot 7 + 0$ so $252 \operatorname{div} 7 = 36$ and $252 \bmod 7 = 0$

b. $1398 = 107 \cdot 13 + 7$ so $1398 \operatorname{div} 13 = 107$ and $1398 \bmod 13 = 7$

c. $-21 = -1 \cdot 33 + 12$ so $-21 \operatorname{div} 33 = -1$ and $-21 \bmod 33 = 12$

d. $-457 = -21 \cdot 22 + 5$ so $-457 \operatorname{div} 22 = -21$ and $-457 \bmod 22 = 5$

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. $(1302^3 + 4505^2) \bmod 10$

Solution: Using the rules for arithmetic operations modulo n in Lesson 2.5:

a. Arithmetic in $\mathbb{Z}_{20}$ is the same as $\bmod 20$, so we get $9 \times 3 \bmod 20 = 27 \bmod 20 = 7$

b. $15^{26} \bmod 7 = (15 \bmod 7)^{26} \bmod 7 = (1)^{26} \bmod 7 = 1 \bmod 7 = 1$

c. $(352 \cdot 407) \bmod 50 = [(352 \bmod 50) \cdot (407 \bmod 50)] \bmod 50 = (2 \cdot 7) \bmod 50 = 14 \bmod 50 = 14$

d. $(1302^3 + 4505^2) \bmod 10 = [(1302^3 \bmod 10) + (4505^2 \bmod 10)] \bmod 10$

$= [((1302 \bmod 10)^3 \bmod 10) + ((4505 \bmod 10)^2 \bmod 10)] \bmod 10$

$= [(2^3 \bmod 10) + (5^2 \bmod 10)] \bmod 10$

$= [(8 \bmod 10) + (25 \bmod 10)] \bmod 10 = [8 + 5] \bmod 10 = 13 \bmod 10 = 3$

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

Solution: You can use the box labeled "Small factors" in Lesson 2.9, to reduce the number of potential factors to check.

1. Prime
2. Not prime: $481 = 13 \cdot 37$
3. Prime

4. Not prime: $2021 = 43 \cdot 47$

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

Solution: To find the GCD, use the Euclidean Algorithm in Lesson 2.10. To find the linear combination, follow the Extended Euclidean Algorithm in Lesson 2.11. For the multiplicative inverse, see Lesson 2.12: If $\gcd(x, y) = 1$, then the multiplicative inverse exists and can be read off of the linear combination as the coefficient for value x. If $\gcd(x, y) \neq 1$, then the multiplicative inverse does not exist.

a. (i) $\gcd(45, 55) = 5$

(ii) $5 = 5 \cdot 45 - 4 \cdot 55$

(iii) $\gcd(45, 55) \neq 1$, so the inverse of $45 \bmod 55$ does not exist

b. (i) $\gcd(51, 72) = 3$

(ii) $3 = 5 \cdot 72 - 7 \cdot 51$

(iii) $\gcd(51, 72) \neq 1$, so the inverse of $51 \bmod 72$ does not exist

c. (i) $\gcd(39, 44) = 1$

(ii) $1 = 8 \cdot 44 - 9 \cdot 39$

(iii) $\gcd(39, 44) = 1$, so the inverse of $39 \bmod 44$ is the coefficient of 39 in the linear combination. That is, the inverse of 39 is $-9 \bmod 44 = 35$.

d. (i) $\gcd(324, 431) = 1$

(ii) $1 = 145 \cdot 324 - 109 \cdot 431$

(iii) $\gcd(324, 431) = 1$, so the inverse of $324 \bmod 431$ is the coefficient of 324 in the linear combination. That is, the inverse of 324 is 145.

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. $(2B8E)_{16}$

c. $(101010)_2$

Solution:

a. $(523)_8 = 5 \cdot 8^2 + 2 \cdot 8^1 + 3 \cdot 8^0 = 339$

b. Recall in hexadecimal (base 16) that B $= 11$ and E $= 14$.
$(2B8E)_{16} = 2 \cdot 16^3 + 11 \cdot 16^2 + 8 \cdot 16^1 + 14 \cdot 16^0 = 11150$

c. $(101010)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 42$

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

a. $(7\text{E}0)_{16}$

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

c. $(1100100101100000)_2$

d. $(11010011101111110101)_2$

Solution: Converting binary to hex (or vice versa) can be accomplished quickly with the following table, found in 2.15.

Decimal	0	1	2	3	4	5	6	7
Binary	0000	0001	0010	0011	0100	0101	0110	0111
Hex	0	1	2	3	4	5	6	7

Decimal	8	9	10	11	12	13	14	15
Binary	1000	1001	1010	1011	1100	1101	1110	1111
Hex	8	9	A	B	C	D	E	F

a. $(7\text{E}0)_{16} = (11111100000)_2$

b. $(25\text{DAA})_{16} = (100101110110101010)_2$

c. $(1100100101100000)_2 = (\text{C960})_{16}$

d. $(11010011101111110101)_2 = (\text{D3BF5})_{16}$

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

Solution: Each of these can be accomplished by repeatedly applying mod and div, as described by the algorithm in Lesson 2.16.

a. $716 = (10331)_5$

b. $500 = (1313)_7$

c. $1,000,000 = (\text{F4240})_{16}$

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 $5^{44} \bmod 89$.

Solution: These exercises are completed using modular exponentiation found in Lesson 2.19. You can also watch this video on modular exponentiation.

a. Remainder is 16.

Recall that finding the remainder is the same as finding a mod value. We will compute $3^{50} \bmod 23$.

Start by writing 50 in its base 2 expansion. You can convert to binary first if that helps: $50 = (110010)_2 = 2^5 + 2^4 + 2^1$. Use this to rewrite the 50 and use a property of exponents.

$$3^{50} = 3^{2^5+2^4+2^1} = 3^{2^5} \cdot 3^{2^4} \cdot 3^{2^1}$$

You can calculate the following table with successive squaring.

n	0	1	2	3	4	5
$3^{2^n} \bmod 23$	3	9	12	6	13	8

Then, we have

$$3^{50} \bmod 23 \equiv 3^{2^5} \cdot 3^{2^4} \cdot 3^{2^1} \bmod 23 \equiv 8 \cdot 13 \cdot 9 \bmod 23 \equiv 16$$

b. Remainder is 6.

Similar process as part a. Notice that $117 = (1110101)_2 = 2^6 + 2^5 + 2^4 + 2^2 + 2^0$ We can calculate the following table with successive squaring.

n	0	1	2	3	4	5	6
$7^{2^n} \bmod 11$	7	5	3	9	4	5	3

So we have that

$$7^{117} \bmod 11 \equiv 7^{2^6} \cdot 7^{2^5} \cdot 7^{2^4} \cdot 7^{2^2} \cdot 7^{2^0} \bmod 11 \equiv 3 \cdot 5 \cdot 4 \cdot 3 \cdot 7 \bmod 11 \equiv 6$$

c. $5^{44} \bmod 89 \equiv 1$

Similar process to part a. Note that $44 = (101100)_2 = 2^5 + 2^3 + 2^2$. We can calculate the following table with successive squaring

n	0	1	2	3	4	5
$5^{2^n} \bmod 89$	5	25	2	4	16	78

Therefore we have that

$$5^{44} \bmod 89 \equiv 5^{2^5} \cdot 5^{2^3} \cdot 5^{2^2} \bmod 89 \equiv 78 \cdot 4 \cdot 2 \bmod 89 \equiv 1$$

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

Solution: If we want to know the last 4 bits of the binary representation, we really just want to know what the number is mod 16. First we have to find the binary representation of 1402 in order to do the successive squaring method.

$$1402 = 2^{10} + 2^8 + 2^6 + 2^5 + 2^4 + 2^3 + 2^1$$

Now can make the table using successive squaring

n	0	1	2	3	4	5	6	7	8	9	10
$3^{2^n} \pmod{16}$	3	9	1	1	1	1	1	1	1	1	1

Putting it all together we get that

$$3^{1402} \equiv 3^{2^1} \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^5} \cdot 3^{2^6} \cdot 3^{2^8} \cdot 3^{2^{10}} \equiv 9 \pmod{16}$$

Therefore the last 4 bits of 3^{1402} are 1001.

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.

Solution: Letters are represented by 2 digits, so it may be easier to see as

$$10 - 21 - 20 - 26 - 22 - 07 - 20 - 15 - 09$$

Using the scheme described gives

$$D - O - N - T - P - A - N - I - C$$

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"

Solution:

a. $N = p \cdot q = 667$ and $\phi = (p-1)(q-1) = 616$.

b. The only condition for picking a value of e is that $\gcd(e, \phi) = 1$. Between 60 and 80 there are 8 such values: 61, 65, 67, 69, 71, 73, 75, and 79. Any one of these would be considered correct. For good practice (more steps) of the Extended Euclidean Algorithm in part c, consider using a value for e that is 69 or higher.

c. In order to determine d, find the inverse of $e \bmod \phi$. The process is the Extended Euclidean Algorithm. The answer depends on your choice of e and is listed in the table below.

d. To encrypt a plaintext message, m, this formula will produce c, the cyphertext: $c = m^e \bmod N$ as shown in Lesson 2.23. The answer depends on your choice of e and is listed in the table below.

e	d	c
61	101	10
65	417	664
67	331	659
69	125	201
71	295	536
73	481	540
75	115	106
79	39	235

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 $N = 6077, e = 987$

Solution:

a. Start by finding the prime factorization of $N = 319 = 11 \cdot 29$. Then $\phi = (11 - 1)(29 - 1) = 10 \cdot 28 = 280$. Using the Extended Euclidian Algorithm, find the inverse of $17 \pmod{280}$ to get $d = 33$.

b. i This key is invalid since $N = 17 \cdot 29 \cdot 101$ is the product of 3 primes, not 2 primes.

ii This is valid since $N = 17 \cdot 37$ is the product of two primes, $\phi = 16 \cdot 36 = 576$ and we calculate that $\gcd(576, 421) = 1$. To find a private key we need to find the multiplicative inverse of $421 \pmod{576}$. Using the Extended Euclidean algorithm we get

$$1 = 201 \cdot 576 - 275 \cdot 421$$

Therefore, a private key would be $d = -275 \bmod 576 = 301$.

iii This key is invalid. $N = 59 \cdot 103$ is the product of two primes, but then $\phi = 58 \cdot 102 = 5916$ is not coprime with 987, since $\gcd(987, 5916) = 3$.