Concepts:

- Define the concepts "a divides b" or "b is divisible by a" or "b is a multiple of a."
- Prove simple statements involving divisibility.
- Define and perform the Division Algorithm.
- Identify the proper range of a remainder in the division algorithm.
- Evaluate "div" and "mod" binary operators on integers.
- Define and evaluate "a mod m."
- Define the concept "a congruent b (mod m)."
- Perform modular arithmetic on expressions involving additions and multiplications.
- Perform fast modular exponentiation to evaluate a^{2^k} mod m expressions.

Problems:

1. Fill in the blanks in the statements below:

   (a) Let a and d are integers with $d \neq 0$. We say d divides a if ...

   (b) Let a be an integer and d be a positive integer. The Division Algorithm states that ...

   (c) Let a be an integer and m be a positive integer. a mod m represents ...

   (d) Let a be an integer and m be a positive integer. a div m represents ...

   (e) Let a and b be integers and m be an integer greater than 1. Then $a \equiv b \bmod m$ means that ...

   (f) Let a and b be integers and m be an integer greater than 1. Then $(a + b) \bmod m = \ldots$

   (g) Let a and b be integers and m be an integer greater than 1. Then $(a \cdot b) \bmod m = \ldots$

   (h) Let a, m and k be positive integers such that $m \geq 2$. What computationally efficient procedure would you apply to calculate a^{2^k} mod m?

2. Check whether the following statements are true or false.

   (a) Assume $a \neq 0$ and b are integers. The notation $a|b$ means "a divides b." That is, there is an integer q such that $b = qa$.

   (b) The following statements are equivalent:

   "a divides b", "b is a multiple of a", "a is a factor of b" and "a is a divisor of b."

3. Check whether the following statements are true or false. If you think the statement is true, then give a short proof. If you think the statement is false, then give a counter example.

(a) Assume $a \neq 0$ and b are integers. If $a|b$, then $a|b^2$.

(b) Assume $a \neq 0$ and b are integers. If $a|b^2$, then $a|b$.

(c) Assume $a \neq 0$, b and c are integers. If $a|b$ and $b|c$, then $a|c$.

4. Find $(234 \bmod 43 + 213 \bmod 43) \bmod 43$.

5. Find two different integers a and b, such that $a \bmod 47 = 23$, $b \bmod 47 = 23$, and both a and b are negative.

6. Use modular arithmetic to find $(12345678 \cdot 9056348992391 + 3^{123456754}) \bmod 4$. Show your work. Don't multiply 12345678 and 9056348992391 together.

   Hint: In your calculation apply the theorems below:

   - $(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$
   - $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$
   - $a^n \bmod m = ((a \bmod m)^n) \bmod m$

7. Find the smallest positive integer a such that $a \bmod 3 = 2$ and $a \bmod 5 = 3$.

8. Without using a calculator find $5^8 \bmod 7$ in two ways:

   (a) First multiply two 5's together and evaluate the product mod 7. Multiply this value by 5 and evaluate it mod 7. Keep repeating this procedure until you receive $5^8 \bmod 7$. How many multiplications did you use in this procedure?

   (b) Use fast modular exponentiation. How many squaring steps did you use in this algorithm?

9. (a) Find the smallest positive integer n such that $3^n \bmod 11 = 1$.

   (b) Use the previous result, modular arithmetic and laws of exponents to find $3^{236} \bmod 11$.

   (c) Find $3^n \bmod 11$ for the following values of n:
   - when $n \bmod 5 = 0$
   - when $n \bmod 5 = 1$
   - when $n \bmod 5 = 2$
   - when $n \bmod 5 = 3$
   - when $n \bmod 5 = 4$

10. Use fast modular exponentiation to calculate $2^{1024} \bmod 13$. How many "squaring steps" were performed in the algorithm?

11. Prove that a positive integer n is divisible by 3 if and only if the sum of the digits of n (in decimal representation) is divisible by 3.

    For example: you can test if 234588 is divisible by 3 by adding its digits. Since $2 + 3 + 4 + 5 + 8 + 8 = 30$ is divisible 3, 234588 is also divisible by 3.

    (Hint: Let $n = a_d 10^d + a_{d-1}10^{d-1} + a_{d-2}10^{d-2} + \cdots + a_1 10 + a_0$ be n's decimal expansion. Use modular arithmetic to find $n \bmod 3$ in terms of the sum of the digits a_i, $i = 0, 1, 2, \ldots, d$).

Solutions:

1. Fill in the blanks in the statements below:

   (a) Let a and d are integers with $d \neq 0$. We say d divides a if there exists an integer k such that $a = k \cdot d$.

   (b) Let a be an integer and d be a positive integer. The Division Algorithm states that there exist unique integers q and r such that $a = qd + r$ where $0 \leq r < d$. The integer a is called the dividend, d is called the divisor, q is called the quotient and r is called the remainder.

   (c) Let a be an integer and m be a positive integer. $a \bmod m$ represents r the remainder in the Division Algorithm when a is divided by m.

   (d) Let a be an integer and m be a positive integer. Then a div m represents q the quotient in the Division Algorithm when a is divided by m. In fact $q = \lfloor \frac{a}{m} \rfloor$.

   (e) Let a and b be any two integers and m be an integer greater than 1. Then $a \equiv b \pmod{m}$ means that m divides $a - b$. Equivalently, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

   (f) Let a and b be any two integers and m be an integer greater than 1. Then $(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$

   (g) Let a and b be integers and m be an integer greater than 1. Then $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

   (h) Let a, m and k be positive integers such that $m \geq 2$. What procedure would you apply to calculate $a^{2^k} \bmod m$?

   We would use fast modular exponentiation to calculate $a^{2^k} \bmod m$. The successive squaring of a will result in a^{2^k} in k steps. After each squaring we reduce the answer modulo m, and in the next squaring step we use this reduced value.

2. Check whether the following statements are true or false.

   (a) Assume $a \neq 0$ and b are integers. The notation $a|b$ means "a divides b." That is, there is an integer q such that $b = qa$.

   True. Note that the notation $a|b$, means that a divides b. That is, $\frac{b}{a}$ is an integer.

   (b) The following statements are equivalent:

   "a divides b", "b is a multiple of a", "a is a factor of b" and "a is a divisor of b."

   True. All of these mean that $\frac{b}{a}$ is an integer.

3. Check whether the following statements are true or false. If you think the statement is true, then give a short proof. If you think the statement is false, then give a counter example.

(a) Assume $a \neq 0$ and b are integers. If $a|b$, then $a|b^2$.

True. Assume $a \neq 0$ and b are integers such that a divides b. By the definition of divisibility, $b = k \cdot a$ for some integer k. Multiplying both sides of the equation by b, we obtain $b^2 = (kb) \cdot a$. Since kb is an integer, a divides b by the definition of divisibility.

(b) Assume $a \neq 0$ and b are integers. If $a|b^2$, then $a|b$.

False. Let $a = 12$ and $b = 6$. Then a divides b^2 but a does not divide b.

(c) Assume $a \neq 0$, $b \neq 0$, and c are integers. If $a|b$ and $b|c$, then $a|c$.

True. Assume $a \neq 0$, $b \neq 0$, and c are integers such that a divides b and b divides c. By the definition of divisibility, $b = k \cdot a$ and $c = \ell \cdot b$ for some integers k, ℓ. Substituting $b = k \cdot a$ into $c = \ell \cdot b$, we obtain $c = (\ell k) \cdot a$. Since ℓk is an integer, a divides c by the definition of divisibility.

4. Find $(234 \bmod 43 + 213 \bmod 43) \bmod 43$.

$(234 \bmod 43 + 213 \bmod 43) \bmod 43 = (19 + 41) \bmod 43 = 17$.

5. Find two different integers a and b, such that $a \bmod 47 = 23$ and $b \bmod 47 = 23$ and both a and b are negative.

Any integer a which gives a remainder 23 when it is divided by 47, can be written in the form of $n = 47k+23$ for some integer k. To obtain two negative integers satisfying the required property, we can choose $k = -1,\ -2$. Thus, $-24,\ -71$ are two negative numbers such that $-24 \bmod 47 = 23$ and $-71 \bmod 47 = 23$.

6. Use modular arithmetic to find $(12345678 \cdot 9056348992391 + 3^{123456754}) \bmod 4$. Show your work. Don't multiply 12345678 and 9056348992391 together.

Hint: In your calculation apply the theorems below:

- $(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$
- $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$
- $a^n \bmod m = ((a \bmod m)^n) \bmod m$

Since $3^{123456754} \bmod 4 = (3^2)^{61728377} \bmod 4 = 9^{61728377} \bmod 4 = ((9 \bmod 4)^{61728377}) \bmod 4 = 1$,

$$(12345678 \cdot 9056348992391 + 3^{123456754}) \bmod 4 = ((12345678 \bmod 4) \cdot (9056348992391 \bmod 4) +$$
$$3^{123456754} \bmod 4) \bmod 4 = ((2 \cdot 3) + 1) \bmod 4 = 3.$$

7. Find the smallest positive integer a such that $a \bmod 3 = 2$ and $a \bmod 5 = 3$.

Any integer a with the property that $a \bmod 3 = 2$ can be written in the form $a = 3k + 2$ for some integer k. We need to find the smallest integer k such that $a = 3k + 2$ is positive and $a \bmod 5 = 3$. The smallest such k is $k = 2$, which gives $a = 8$.

8. Without using a calculator find $5^8 \bmod 7$.

(a) First multiply two 5's together and evaluate the product mod 7. Multiply this value by 5 and evaluate it mod 7. Keep repeating this procedure until you receive 5^8 mod 7. How many multiplications did you use in this procedure?

We will multiply two factors at a time and evaluate it mod 7.
$(\underbrace{5\cdot 5}_{=4}\cdot 5\cdot 5\cdot 5\cdot 5\cdot 5\cdot 5) \bmod 7 = (\underbrace{4\cdot 5}_{=6}\cdot 5\cdot 5\cdot 5\cdot 5\cdot 5) \bmod 7 = (\underbrace{6\cdot 5}_{=2}\cdot 5\cdot 5\cdot 5\cdot 5) \bmod 7 =$
$(\underbrace{2\cdot 5}_{=3}\cdot 5\cdot 5\cdot 5) \bmod 7 = (\underbrace{3\cdot 5}_{=1}\cdot 5\cdot 5) \bmod 7 = 4.$
7 multiplications were use in the procedure.

(b) Use fast modular exponentiation. How many squaring steps did you use in this algorithm?

We perform the algorithm.

$$5^{2^0} \bmod 7 = 5^1 \bmod 7 = 5$$

$$5^{2^1} \bmod 7 = 5^2 \bmod 7 = 4$$

$$5^{2^2} \bmod 7 = 4^2 \bmod 7 = 2$$

$$5^{2^3} \bmod 7 = 2^2 \bmod 7 = 4$$

Thus, $5^{2^3} \bmod 7 = 4$. The algorithm used 3 squaring steps.

9. (a) Find the smallest positive integer n such that $3^n \bmod 11 = 1$.

We use a trial method.
$3^1 \bmod 11 = 3, 3^2 \bmod 11 = 9, 3^3 \bmod 11 = 5, 3^4 \bmod 11 = 4, 3^5 \bmod 11 = 1$. Thus, $n = 5$ is the smallest positive integer n for which $3^n \bmod 11 = 1$. Now, the remainders will repeat in a cycle $3, 9, 5, 4, 1$.

(b) Use the previous result, modular arithmetic and laws of exponents to find $3^{236} \bmod 11$.

Since $236 = 5\cdot 47 + 1$, $3^{236} \bmod 11 = 3^{5\cdot 47+1} \bmod 11 = (3^{5\cdot 47}\cdot 3^1) \bmod 11 = (((3^5 \bmod 11)^{47} \bmod 11)\cdot (3 \bmod 11)) \bmod 11 = (1\cdot 3) \bmod 11 = 3$.
Note that we divided the exponent 236 by 5, because 5 is the smallest smallest positive integer n such that $3^n \bmod 11 = 1$.

(c) Find $3^n \bmod 11$ for the following values of n:

- when $n \bmod 5 = 0$
- when $n \bmod 5 = 1$
- when $n \bmod 5 = 2$
- when $n \bmod 5 = 3$
- when $n \bmod 5 = 4$

By the Division Algorithm any exponent n can be written in the form of $n = 5k + r$ where k and r are non-negative integers such that $0 \le r < 5$. Since $3^5 \bmod 11 = 1$, $3^n \bmod 11 = 3^{5k+r} \bmod 11 = ((3^5 \bmod 11)^k \cdot (3^r \bmod 11)) \bmod 11 = 3^r \bmod 11$. Thus,

$$3^n \bmod 11 = \begin{cases} 3^0 \bmod 11 = 1 \text{ when } n \bmod 5 = 0 \\ 3^1 \bmod 11 = 3 \text{ when } n \bmod 5 = 1 \\ 3^2 \bmod 11 = 9 \text{ when } n \bmod 5 = 2 \\ 3^3 \bmod 11 = 5 \text{ when } n \bmod 5 = 3 \\ 3^4 \bmod 11 = 4 \text{ when } n \bmod 5 = 4 \end{cases}$$

10. Use fast modular exponentiation to calculate $3^{1024} \bmod 7$. How many "squaring steps" were performed in this algorithm?

Since $1024 = 2^{10}$, successive squaring of the base 3 will result in 3^{1024} in 10 squaring steps. Now we perform the algorithm.

$$3^{2^0} \bmod 7 = 3^1 \bmod 7 = 3$$

$$3^{2^1} \bmod 7 = 3^2 \bmod 7 = 2$$

In the second step, we obtain the result by squaring 3 and not calculating $3^{2^1} \bmod 7$.

$$3^{2^2} \bmod 7 = 2^2 \bmod 7 = 4$$

In the third step, we obtain the result by squaring 2 and not calculating $3^{2^2} \bmod 7$.

$$3^{2^3} \bmod 7 = 4^2 \bmod 7 = 2$$

In the fourth step, we obtain the result by squaring 4 and not calculating $3^{2^3} \bmod 7$. Thus, the remainders $2,\ 4$ will be repeating in a two-cycle.

$$3^{2^k} \bmod 11 = \begin{cases} 3 \text{ when } k = 0 \\ 2 \text{ when } n \text{ odd} \\ 4 \text{ when } n \text{ even} \end{cases}$$

The exponent is 10 is even, so

$$3^{2^{10}} \bmod 7 = 4.$$

11. Prove that a positive integer n is divisible by 3 if and only if the sum of the digits of n (in decimal representation) is divisible by 3.

For example: you can test if 234588 is divisible by 3 by adding its digits. Since $2+3+4+5+8+8 = 30$ is divisible 3, 234588 is also divisible by 3.

(Hint: Let $n = a_d 10^d + a_{d-1}10^{d-1} + a_{d-2}10^{d-2} + \cdots + a_1 10 + a_0$ be n's decimal expansion. Use modular arithmetic to find $n \bmod 3$ in terms of the sum of the digits a_i, $i = 0, 1, 2, \ldots, d$).

Proof: Let $n = a_d 10^d + a_{d-1}10^{d-1} + a_{d-2}10^{d-2} + \cdots + a_1 10 + a_0$ be n's decimal expansion with $d+1$ digits. Since $10 \bmod 3 = 1$, $n \bmod 3 = (a_d 10^d + a_{d-1}10^{d-1} + a_{d-2}10^{d-2} + \cdots + a_1 10 + a_0) \bmod 3 = (a_d + a_{d-1} + a_{d-2} + \ldots a_1 + a_0) \bmod 3$.

Consequently, $n \bmod 3 = 0$ (i.e., n is divisible by 3) if and only if $(a_d + a_{d-1} + a_{d-2} + \ldots a_1 + a_0) \bmod 3 = 0$ (i.e., the sum of the digits is divisible by 3). ■