1. Find the following:

   (a) Find the values of $\overline{6}+\overline{13}$, $\overline{6}-\overline{13}$, and $\overline{6}\cdot\overline{13}$ in $\mathbb{Z}/11\mathbb{Z}$. Write your answers as $\overline{a}$ where $0 \le a \le 10$.

   - We have $\overline{6}+\overline{13}=\overline{19}=\boxed{\overline{8}}$, $\overline{6}-\overline{13}=\overline{-7}=\boxed{\overline{4}}$, and $\overline{6}\cdot\overline{13}=\overline{78}=\boxed{\overline{1}}$.

   (b) Give the addition and multiplication tables modulo 7. (For ease of writing, you may omit the bars in the residue class notation.)

   -

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

   (c) Find all of the invertible residue classes modulo 7 and their multiplicative inverses.

   - Every nonzero residue class is invertible: explicitly, $\overline{1}^{-1}=\overline{1}$, $\overline{2}^{-1}=\overline{4}$, $\overline{3}^{-1}=\overline{5}$, $\overline{4}^{-1}=\overline{2}$, $\overline{5}^{-1}=\overline{3}$, and $\overline{6}^{-1}=\overline{6}$.

   (d) Give the multiplication table modulo 8. (Again, you may omit the bars.)

   -

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

   (e) Find all of the invertible residue classes modulo 8 and their multiplicative inverses.

   - Modulo 8, only the odd residue classes are invertible, and in fact each one is its own inverse: $\overline{1}^{-1}=\overline{1}$, $\overline{3}^{-1}=\overline{3}$, $\overline{5}^{-1}=\overline{5}$, $\overline{7}^{-1}=\overline{7}$. The other residue classes $\overline{0}$, $\overline{2}$, $\overline{4}$, $\overline{6}$ are not invertible.

   (f) Give the multiplication table modulo 9. (Again, you may omit the bars.)

   -

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{3}$	$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{1}$	$\overline{6}$	$\overline{2}$	$\overline{7}$	$\overline{3}$	$\overline{8}$	$\overline{4}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

   (g) Find all of the invertible residue classes modulo 9 and their multiplicative inverses.

   - Modulo 9, the invertible residue classes are $\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}$: $\overline{1}^{-1}=\overline{1}$, $\overline{2}^{-1}=\overline{5}$, $\overline{4}^{-1}=\overline{7}$, $\overline{5}^{-1}=\overline{2}$, $\overline{7}^{-1}=\overline{4}$, $\overline{8}^{-1}=\overline{8}$. The other residue classes $\overline{0}$, $\overline{3}$, $\overline{6}$ are not invertible.

2. Find the multiplicative inverse of each residue class $\overline{a}$ modulo m, or explain why it does not exist.

   (a) The residue class $\overline{7}$ modulo 10.

   - Via the Euclidean algorithm we can compute $3 \cdot 7 - 2 \cdot 10 = 1$ so 7 and 10 are relatively prime. So the inverse exists.
   - Reducing the Euclidean algorithm calculation modulo 10 yields $3 \cdot 7 \equiv 1 \pmod{10}$, so $\overline{3} \cdot \overline{7} = \overline{1}$ modulo 10. Hence $\overline{7}^{-1} = \boxed{\overline{3}}$ mod 10.

   (b) The residue class $\overline{14}$ modulo 49.

   - We can see that 14 and 49 are not relatively prime since their gcd is 7, so $\overline{14}$ $\boxed{\text{does not have}}$ a multiplicative inverse modulo 49.

   (c) The residue class $\overline{16}$ modulo 49.

   - Via the Euclidean algorithm we can compute $1 \cdot 49 - 3 \cdot 16 = 1$ so 16 and 49 are relatively prime. So the inverse exists.
   - Reducing the Euclidean algorithm calculation modulo 49 yields $\overline{-3} \cdot \overline{16} = \overline{1}$ so the multiplicative inverse of $\overline{16}$ is $\boxed{\overline{-3} = \overline{46}}$ mod 49.

   (d) The residue class $\overline{5}$ modulo 2024.

   - Via the Euclidean algorithm we can compute $405 \cdot 5 - 2024 = 1$ so 5 and 2024 are relatively prime. So the inverse exists.
   - Reducing the Euclidean algorithm calculation modulo 49 yields $\overline{405} \cdot \overline{5} = \overline{1}$ so the multiplicative inverse of $\overline{5}$ is $\boxed{\overline{405}}$ mod 2024.

---

3. Suppose a, b, c, d, m are integers and $m > 0$. Prove the following properties of modular arithmetic:

   (a) If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$ for any $c > 0$.

   - Suppose $a \equiv b \pmod{m}$. Then by definition, $m|(b-a)$. So by properties of divisibility, we see that mc divides $(b-a)c = bc - ac$.
   - So by definition, this means $ac \equiv bc \pmod{mc}$ as claimed. (Note that $c > 0$ is needed only because the modulus mc is required to be positive.)

   (b) If $d|m$ and $d > 0$, then $a \equiv b \pmod{m}$ implies $a \equiv b \pmod{d}$.

   - Suppose $a \equiv b \pmod{m}$. Then by definition, $m|(b-a)$. But now because $d|m$, by properties of divisibility we see that $d|(b-a)$.
   - So by definition, this means $a \equiv b \pmod{d}$ as claimed.

   (c) If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$ for every positive integer n.

   - Induction on n. The base case $n = 1$ is simply $a \equiv b \pmod{m}$, which is given.
   - For the inductive step suppose $a^n \equiv b^n \pmod{m}$. Multiplying this congruence by $a \equiv b \pmod{m}$ yields $a^{n+1} \equiv b^{n+1} \pmod{m}$, which establishes the inductive step.

   (d) Prove that the operation $+$ is commutative modulo m: namely, that $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ for any $\overline{a}$ and $\overline{b}$.

   - By definition of residue class addition we have $\overline{a} + \overline{b} = \overline{a+b}$, and also $\overline{b} + \overline{a} = \overline{b+a}$.
   - But by the commutative property [I2] in $\mathbb{Z}$, we know that $a + b = b + a$, so the associated residue classes $\overline{a+b}$ and $\overline{b+a}$ are also equal. Hence $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$ as claimed.

   (e) Prove that the operation $\cdot$ is associative modulo m: namely, that $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$ for any $\overline{a}$, $\overline{b}$, and $\overline{c}$.

   - By definition of residue class multiplication we have $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{b \cdot c} = \overline{a \cdot (b \cdot c)}$ and also $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a \cdot b} \cdot \overline{c} = \overline{(a \cdot b) \cdot c}$.
   - But by the associative property [I5] in $\mathbb{Z}$, we know that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, so the associated residue classes $\overline{a \cdot (b \cdot c)}$ and $\overline{(a \cdot b) \cdot c}$ are also equal. Hence $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{b \cdot c} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot b} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$ as claimed.

   (f) Prove that the residue class $\overline{1}$ is a multiplicative identity modulo m, namely, that $\overline{1} \cdot \overline{a} = \overline{a}$ for any $\overline{a}$.

   - By definition of residue class multiplication and the identity property [I7] we see $\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a}$, as claimed, since $1 \cdot a = a$ as integers.

---

4. The goal of this problem is to discuss modular exponentiation, which is frequently used in cryptography. If n is a positive integer, we define $\overline{a}^n \pmod{m}$ to be the n-term product $\underbrace{\overline{a} \cdot \overline{a} \cdot \dots \cdot \overline{a}}_{n \text{ terms}} \pmod{m}$. By problem 3c, one has $\overline{a}^n = \overline{a^n}$ (i.e., the nth power of the residue class $\overline{a}$ is the residue class of the nth power a^n).

   (a) Find the residue classes $\overline{2}^2$, $\overline{2}^3$, $\overline{2}^4$, $\overline{2}^5$, $\overline{2}^6$, $\overline{3}^2$, $\overline{3}^3$, $\overline{3}^4$, $\overline{3}^5$, and $\overline{3}^6 \pmod{10}$. (Write your answers as residue classes $\overline{r}$ where $0 \le r \le 9$.)

      - We simply calculate $\overline{2}^2 = \boxed{\overline{4}}$, $\overline{2}^3 = \boxed{\overline{8}}$, $\overline{2}^4 = \overline{16} = \boxed{\overline{6}}$, $\overline{2}^5 = \overline{32} = \boxed{\overline{2}}$, $\overline{2}^6 = \overline{64} = \boxed{\overline{4}}$.
      - Likewise, $\overline{3}^2 = \boxed{\overline{9}}$, $\overline{3}^3 = \overline{27} = \boxed{\overline{7}}$, $\overline{3}^4 = \overline{81} = \boxed{\overline{1}}$, $\overline{3}^5 = \overline{243} = \boxed{\overline{3}}$, $\overline{3}^6 = \overline{729} = \boxed{\overline{9}}$.

   (b) It is natural to think that if $n_1 \equiv n_2 \pmod{m}$, then $a^{n_1} \equiv a^{n_2} \pmod{m}$; i.e., that exponents "can also be reduced mod m". Show that this is incorrect by verifying that 2^2 is not congruent to 2^7 modulo 5.

      - We calculate $2^2 \equiv 4$ modulo 5, while $2^7 = 128 \equiv 3$ modulo 5. They are not congruent.

   (c) Show in fact that if $a \not\equiv 0$ modulo 5, then $a^4 \equiv 1 \pmod 5$. Deduce that $a^{n_1} \equiv a^{n_2} \pmod 5$ whenever $n_1 \equiv n_2 \pmod 4$, so that the exponents actually behave "modulo 4". [Hint: For the first part, test the 4 possible residue classes for a. For the second part, explain why $a^{4k} \equiv 1 \pmod 5$ for any k.]

      - Since there are only 4 nonzero residue classes modulo 5, we simply check them all.
      - We have $1^4 \equiv 1 \pmod 5$, $2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, and $4^4 = 256 \equiv 1 \pmod 5$. So the result holds in all cases.
      - For the second part, we just showed that $a^4 \equiv 1 \pmod 5$ for any nonzero a. Taking the kth power then yields $a^{4k} \equiv 1^k \equiv 1 \pmod 5$.
      - Now, if $n_1 \equiv n_2 \pmod 4$, then $n_2 - n_1 = 4k$ for some integer k which (by interchanging n_1, n_2 if needed) we may assume is nonnegative. We then have $a^{n_2} = a^{n_1+4k} = a^{n_1} \cdot (a^4)^k \equiv a^{n_1} \cdot 1^k = a^{n_1} \pmod 5$, as claimed.

Now suppose we want to find the remainder when we divide 2^{516} by 61. Here is an efficient approach: compute the values $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 16^2 \equiv 12$, $2^{16} \equiv 12^2 \equiv 22$, $2^{32} \equiv 22^2 \equiv -4$, $2^{64} \equiv 16$, $2^{128} \equiv 12$, $2^{256} \equiv 22$, $2^{512} \equiv 57$ modulo 61 by squaring each previous term and reducing. Then simply evaluate $2^{516} = 2^{512} \cdot 2^4 \equiv 57 \cdot 16 \equiv 58$ (modulo 61), so the remainder is 58.

   (e) Use the method described above to find the remainder when 3^{261} is divided by 43.

      - We compute $3^1 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 81 \equiv -5$, $3^8 \equiv 25$, $3^{16} \equiv 625 \equiv 23$, $3^{32} \equiv 529 \equiv 13$, $3^{64} \equiv 169 \equiv -3$, $3^{128} \equiv (-3)^2 \equiv 9$, $3^{256} \equiv -5$.
      - Then $3^{261} = 3^{256} \cdot 3^4 \cdot 3^1 \equiv (-5) \cdot (-5) \cdot 3 \equiv 75 \equiv 32$. Therefore, the remainder when 3^{261} is divided by 43 is $\boxed{32}$.

   - <u>Remark</u>: Efficient calculations with modular exponentiation are a fundamental part of the RSA cryptosystem, which is still in wide use today.

---

5. Let p be a prime. The goal of this problem is to prove that $a^p \equiv a \pmod{p}$ for every integer a, which is a result known as Fermat's Little Theorem.

   (a) Show that the binomial coefficient $\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}$ is divisible by p for each integer k with $0 < k < p$.

      - If $0 < k < p$ then $\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}$ has a factor of p in the numerator (from the $p!$) but neither $k!$ nor $(p-k)!$ has a factor of p because p is prime and the only terms in $k!$ and $(p-k)!$ are integers less than p.
      - Hence the numerator is divisible by p but the denominator is not, so the quotient divisible by p.

   (b) Prove that $a^p \equiv a \pmod{p}$ for every positive integer a.

      - Fix p and use induction on a. The base case $a = 1$ is trivial since clearly $1^p \equiv 1 \pmod{p}$.
      - For the inductive step, suppose $a^p \equiv a \pmod{p}$.
      - Then $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + \binom{p}{p}1$ by the binomial theorem.
      - By part (a), each of the middle terms is divisible by p, and so we have $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$ by the inductive hypothesis. This establishes the inductive step so by induction the result holds for all positive integers a.

   (c) Show in fact that $a^p \equiv a \pmod{p}$ for all integers a. [Hint: The value of $a^p - a$ mod p only depends on what residue class a lies in mod p.]

      - For a fixed p, the value of $a^p - a$ mod p only depends on the value of a mod p, since if $a \equiv b \pmod{p}$ then $a^p - a \equiv b^p - b \pmod{p}$.
      - So since (b) establishes that $a^p - a$ is 0 modulo p for $a = 0, 1, 2, \ldots, p-1$ (which represent all p possible residue classes for a), in fact $a^p - a$ is 0 modulo p for all integers a.

---

6. The goal of this problem is to establish a simple way to show large integers are composite without finding an explicit factorization.

   (a) Show that if there exists an integer a such that $a^m \not\equiv a \pmod{m}$, then m is composite. [Hint: The result of problem 5 states that if p is prime, then $a^p \equiv a \pmod{p}$ for all integers a.]

      - Fermat's little theorem, in problem 5, states "If p is prime, then $a^p \equiv a \pmod{p}$ for all integers a".
      - Taking the contrapositive yields "If there exists an integer a with $a^p \not\equiv a \pmod{p}$, then p is not prime".
      - Changing the variable from p to m yields the desired result immediately.

   (b) Given that $2^{23381} \equiv 9352 \pmod{23381}$, what can be concluded about whether 23381 is prime or composite?

      - With $a = 2$ and $m = 23381$, since $a^m \not\equiv a \pmod{m}$, part (a) implies that 23381 is composite.

   (c) Given that $2^{23377} \equiv 2 \pmod{23377}$, what can be concluded about whether 23377 is prime or composite?

      - The result of part (a) is *not* an if-and-only-if statement. Since $2^{23377} \equiv 2 \pmod{23377}$, the hypothesis of part (a) does not apply, and therefore we cannot make any conclusion about whether 23377 is prime or composite. (In fact, $23377 = 97 \cdot 241$ is composite!)

   - Remark: The powers in parts (b) and (c) can be calculated quickly using the method discussed in problem 4(e).
