---

1. The goal of this problem is to demonstrate that the uniqueness of integer prime factorizations is not as obvious as it may seem. Let S be a nonempty set of positive integers, and define an <u>S-prime</u> to be an element $p \in S$ such that there do not exist $a, b \in S$ such that $ab = p$ and $1 < a, b < p$. (If S is the set of all positive integers, then this definition reduces to the usual one for prime numbers.) Let $E = \{2, 4, 6, 8, 10, \dots\}$ be the set of even positive integers and let $R = \{1, 5, 9, 13, 17, \dots\}$ be the set of positive integers congruent to 1 modulo 4.

   (a) Which of 2, 4, 6, 8, 10, 12, 14, and 16 are E-primes?

   - We have $4 = 2 \cdot 2$, $8 = 2 \cdot 4$, $12 = 2 \cdot 6$, and $16 = 2 \cdot 8$ so these elements are not E-primes.
   - On the other hand, we cannot factor 2, 6, 10, or 14 as the product of two elements of E, since the product of two elements of E is always divisible by 4. So these elements are E-primes.

   (b) For a positive integer n, when is $2n \in E$ an E-prime? Briefly justify your answer.

   - Based on (a), we claim that $2n$ is an E-prime precisely when n is odd.
   - If $n = 2k$, then $2n = 2 \cdot 2k$ is a factorization of $2n$ as the product of two elements in E, so $2n$ is not an E-prime.
   - On the other hand, if $2n$ is not an E-prime, then $2n = (2a)(2b) = 4ab$ for some integers a, b, so $2n$ is a multiple of 4 hence n is even.

   (c) Show that 60 has two different factorizations as a product of E-primes. Deduce that E does not have unique E-prime factorization.

   - We have $60 = 6 \cdot 10 = 2 \cdot 30$, and by (b) each of 2, 6, 10, and 30 is an E-prime. Since the terms are actually different, and not just rearranged, we see that the factorizations are different, and so E does not have unique E-prime factorization.

   (d) Explain why any prime congruent to 1 modulo 4 (e.g., 5, 13, 17) is an R-prime.

   - Any R-factorization of an integer certainly yields a regular integer factorization. So, any prime number in R (i.e., any prime congruent to 1 modulo 4) cannot have any nontrivial factorization in R, so it is an R-prime.

   (e) Which of the composite numbers 9, 21, 25, 33, 45, 49 are R-primes?

   - We have $25 = 5 \cdot 5$ and $45 = 5 \cdot 9$ so these are not R-primes.
   - However, the only nontrivial integer factorizations of $9 = 3 \cdot 3$, $21 = 3 \cdot 7$, $33 = 3 \cdot 11$, and $49 = 7 \cdot 7$ all involve elements not in R, so these integers have no nontrivial R-factorizations hence are R-primes.

   (f) Find an integer in R that has two different R-prime factorizations. Deduce that R does not have unique R-prime factorization. [Hint: Multiply some of the composite R-primes in (e) together.]

   - Notice that $441 = 21 \cdot 21 = 9 \cdot 49$ has two different R-prime factorizations, as 9, 21, and 49 are R-prime as noted in (e). Thus, R does not have unique R-prime factorization.

---

2. For each element in each ring $\mathbb{Z}[\sqrt{D}]$, determine whether it is a unit and if so find its multiplicative inverse.

   (a) The elements $1 + \sqrt{3}$, $2 + \sqrt{3}$, $3 + \sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$.

   - In $\mathbb{Z}[\sqrt{D}]$, an element is a unit if and only if its norm is ± 1. Note also that the norm of an element here is $N(a + b\sqrt{3}) = a^2 - 3b^2$.
   - Since $N(1 + \sqrt{3}) = 1^2 - 3 \cdot 1^2 = -2$, we see $1 + \sqrt{3}$ $\boxed{\text{is not a unit}}$.
   - Since $N(2 + \sqrt{3}) = 2^2 - 3 \cdot 1^2 = 1$, we see $2 + \sqrt{3}$ $\boxed{\text{is a unit}}$. The norm calculation says $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$, so the multiplicative inverse is $\boxed{2 - \sqrt{3}}$.
   - Since $N(3 + \sqrt{3}) = 3^2 - 3 \cdot 1^2 = 6$, we see $3 + \sqrt{3}$ $\boxed{\text{is not a unit}}$.

   (b) The elements $2 - \sqrt{5}$, $1 + 2\sqrt{5}$, $9 + 4\sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$.

- The norm of an element here is $N(a+b\sqrt{5}) = a^2 - 5b^2$.
- Since $N(2-\sqrt{5}) = 2^2 - 5\cdot 1^2 = -1$, we see $2-\sqrt{5}$ is $\boxed{\text{is a unit}}$. The norm calculation says $(2-\sqrt{5})(2+\sqrt{5}) = -1$, so the multiplicative inverse is $\boxed{-2-\sqrt{5}}$.
- Since $N(1+2\sqrt{5}) = 1^2 - 5\cdot 2^2 = -19$, we see $1+2\sqrt{5}$ is $\boxed{\text{is not a unit}}$.
- Since $N(9+4\sqrt{5}) = 9^2 - 5\cdot 4^2 = 1$, we see $9+4\sqrt{5}$ $\boxed{\text{is a unit}}$. The norm calculation says $(9+4\sqrt{5})(9-4\sqrt{5}) = 1$, so the multiplicative inverse is $\boxed{9-4\sqrt{5}}$.

---

3. Calculate the following:

(a) The values of $\overline{5}+\overline{12}$, $\overline{5}-\overline{12}$, and $\overline{5}\cdot\overline{12}$ in $\mathbb{Z}/14\mathbb{Z}$. Write your answers as $\overline{a}$ where $0 \le a \le 13$.

- We have $\overline{5}+\overline{12} = \overline{17} = \boxed{\overline{3}}$, $\overline{5}-\overline{12} = \overline{-7} = \boxed{\overline{7}}$, and $\overline{5}\cdot\overline{12} = \overline{60} = \boxed{\overline{4}}$.

(b) 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) All of the unit 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) 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) All of the unit 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 units.

---

4. Prove that the following numbers are irrational:

(a) $\sqrt[3]{2}$.

- Suppose $\sqrt[3]{2} = a/b$ for positive integers a and b. Cubing both sides and clearing denominators yields $a^3 = 2b^3$.
- If $a = 2^{a_2}3^{a_3}\cdots p^{a_p}$ and $b = 2^{b_2}3^{b_3}\cdots p^{b_p}$ then $a^3 = 2b^3$ yields $2^{3a_2}3^{3a_3}\cdots p^{3a_p} = 2^{1+3b_2}3^{3b_3}\cdots p^{3b_p}$ and by uniqueness of prime factorizations, all the exponents must agree.
- But this is impossible, since $3a_2 = 1+3b_2$ yields $3(a_2-b_2) = 1$ so that $3|1$, which is clearly false. Thus, $\sqrt[3]{2}$ is irrational.

(b) $\log_3 7$.

- Suppose $\log_3 7 = a/b$ for positive integers a and b. Exponentiating with the base 3 gives $7 = 3^{a/b}$ and now taking bth power of both sides yields $7^b = 3^a$.
- But this is impossible because now the positive integer $n = 7^b = 3^a$ has two different prime factorizations. Thus, $\log_3 7$ is irrational.

---

5. The goal of this problem is to establish the binomial theorem; for no additional charge, we will do this in an arbitrary commutative ring with 1. Define the binomial coefficient $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ for integers $0 \le k \le n$, and note that $\binom{n}{0} = \binom{n}{n} = 1$ for every n. (Recall the definition of $n!$ from homework 1.)

(a) Show that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for every $0 \le k \le n$. Conclude in particular that $\binom{n}{k}$ is always an integer.

- We have $\binom{n}{k} = n \cdot \dfrac{(n-1)!}{k!(n-k)!} = (n-k) \cdot \dfrac{(n-1)!}{k!(n-k)!} + k \cdot \dfrac{(n-1)!}{k!(n-k)!} = \dfrac{(n-1)!}{k!(n-k-1)!} + \dfrac{(n-1)!}{(k-1)!(n-k)!} = \binom{n-1}{k} + \binom{n-1}{k-1}$.
- Then it is an easy induction on n to see $\binom{n}{k}$ is always an integer: the base cases $n = 0$ and $n = 1$ are obvious. For the inductive step, observe that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ is the sum of two integers for any value of k with $1 \le k \le n-1$, and $\binom{n}{0}$ and $\binom{n}{n}$ are also integers.

(b) Suppose that R is a commutative ring with 1. If x and y are arbitrary elements of R, prove that $(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + y^n$ for any positive integer n. [Hint: Use induction on n. You may prefer to use summation notation $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k$ instead.]

- We use induction on n. The base case $n = 1$ is obvious, since $x + y = x + y$.
- For the inductive step, observe that

$$\begin{aligned}
(x+y)^n &= (x+y) \cdot (x+y)^{n-1} \\
&= (x+y) \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k} y^k \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k} y^k + \sum_{j=0}^{n-1} \binom{n-1}{j} x^{n-1-j} y^{j+1} \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k} y^k + \sum_{k=0}^{n-1} \binom{n-1}{k-1} x^{n-k} y^k \\
&= \sum_{k=0}^{n-1} \left[\binom{n-1}{k} + \binom{n-1}{k-1} \right] x^{n-k} y^k = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k
\end{aligned}$$

where we made the substitution $j = k - 1$ in the third equation, and used the result of part (a) in the final step.

---

6. Suppose a, b, c, m are integers and $m > 0$. Prove the following basic properties of modular congruences (these properties are mentioned but not proven in the notes; you are expected to give the details of the proofs):

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

- Suppose $a \equiv b \pmod{m}$. Then by definition, $m|(b-a)$.
- Since $d|m$, by transitivity of divisibility we see $d|(b-a)$. By definition, this means $a \equiv b \pmod{d}$, as claimed.

(b) 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.)

(c) If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for all positive integers n.

- We use induction on n. The base case $n = 1$ is trivial, as $a \equiv b \pmod{m}$ is given.
- For the inductive step, suppose $a^n \equiv b^n \pmod{m}$. Then since $a \equiv b \pmod{m}$, multiplying the congruences yields $a^{n+1} \equiv b^{n+1} \pmod{m}$, as desired.
- Alternatively, if $a \equiv b \pmod{m}$, then $m|(b-a)$ and since $(b-a)|(b^n - a^n)$ we see $m|(b^n - a^n)$ hence $a^n \equiv b^n \pmod{m}$.

---

7. The goal of this problem is to illustrate some applications of modular arithmetic to solving equations in integers (such equations are called Diophantine equations).

(a) If n is a positive integer, show that n^2 is congruent to 0 or 1 modulo 4. [Hint: Square the four possible residue classes modulo 4.]

- There are four possible values for n modulo 4.
- If $n \equiv 0 \pmod{4}$ then $n^2 \equiv 0^2 \equiv 0 \pmod{4}$.
- If $n \equiv 1 \pmod{4}$ then $n^2 \equiv 1^2 \equiv 1 \pmod{4}$.
- If $n \equiv 2 \pmod{4}$ then $n^2 \equiv 2^2 \equiv 0 \pmod{4}$.
- If $n \equiv 3 \pmod{4}$ then $n^2 \equiv 3^2 \equiv 1 \pmod{4}$.
- In all four cases we see n^2 is congruent to 0 or 1 modulo 4.

(b) Show that there do not exist integers a and b such that $a^2 + b^2 = 2023$. [Hint: Work modulo 4.]

- Notice that $2023 \equiv 3 \pmod{4}$. By part (b), the sum of two squares must be congruent to 0, 1, or 2 modulo 4.
- Therefore, 2023 cannot be the sum of two squares, meaning that there do not exist integers a and b such that $a^2 + b^2 = 2023$.

(c) Strengthen (a) by showing that if n is a positive integer, then n^2 is congruent to 0, 1, or 4 modulo 8.

- There are eight possible values for n modulo 8. Testing them all in order, we see that n^2 is congruent to one of $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 1$, $4^2 \equiv 0$, $5^2 \equiv 1$, $6^2 \equiv 4$, $7^2 \equiv 1$ (all modulo 8).
- In all eight cases we see n^2 is congruent to 0, 1, or 4 modulo 8.

(d) Show that there do not exist integers a, b, and c such that $a^2 + b^2 + c^2 = 2023$.

- By part (d), any square is congruent to 0, 1, or 4 modulo 8.
- In particular, if the sum of three squares is odd, then either they are all odd or exactly one is odd.
- Checking the various possibilities, we see that the sum of the squares modulo 8 is congruent to one of $1 + 1 + 1 \equiv 3$, $1 + 0 + 0 \equiv 1$, $1 + 0 + 4 \equiv 5$, or $1 + 4 + 4 \equiv 1$ modulo 8.
- In particular, there is no case in which the sum of the three squares is congruent to 7 modulo 8.
- But now we notice that $2023 \equiv 7 \pmod{8}$, and so by our analysis, 2023 cannot be written as the sum of three squares.
