Problem of the Month

Problem 0: Equations in the integers

September 2025

Suppose a, b, and c are positive integers. In this problem, a *non-negative solution* to the equation $ax + by = c$ is a pair $(x, y) = (u, v)$ of integers with $u \geq 0$ and $v \geq 0$ satisfying $au + bv = c$. For example, $(x, y) = (7, 0)$ and $(x, y) = (3, 3)$ are non-negative solutions to $3x + 4y = 21$, but $(x, y) = (-1, 6)$ is not.

1. Determine all non-negative solutions to $5x + 8y = 120$.
2. Determine the largest positive integer c with the property that there is no non-negative solution to $5x + 8y = c$.

In Questions 3, 4, and 5, a and b are assumed to be positive integers satisfying $\gcd(a, b) = 1$.

3. Determine the largest non-negative integer c with the property that there is no non-negative solution to $ax + by = c$. The value of c should be expressed in terms of a and b.
4. Determine the number of non-negative integers c for which there are exactly 2025 non-negative solutions to $ax + by = c$. As with Question 3, the answer should be expressed in terms of a and b.
5. Suppose $n \geq 1$ is an integer. Determine the sum of all non-negative integers c for which there are exactly n nonnegative solutions to $ax + by = c$. The answer should be expressed in terms of a, b, and n.

Fact: You may find it useful that for integers a and b with $\gcd(a, b) = 1$, there always exist integers x and y such that $ax + by = 1$, though x and y may not be non-negative.

Problem of the Month

Problem 0: Equations in the integers

September 2025

Hint

1. An exhaustive search is a reasonable approach to this problem. It can be made easier if you notice that x must be a multiple of 8 and that y must be a multiple of 5.

2. Find a positive integer c with the property that $ax+by=c$, $ax+by=c+1$, $ax+by=c+2$, $ax+by=c+3$, and $ax+by=c+4$ all have non-negative solutions.

3., 4., 5. As always, it is good to work out a few small examples to try to guess a pattern. It might be useful to understand the set of *all* integer solutions to $ax+by=c$ for fixed a, b, and c with $\gcd(a,b)=1$. Once you do this, you might consider the integer solution $(x,y)=(u,v)$ with u negative but as close to 0 as possible.

Problem of the Month

Solution to Problem 0: Equations in the integers

September 2025

Several times throughout this solution, we will use the following fact: if $\gcd(m, n) = 1$ and km is a multiple of n, then k is a multiple of n. You might want to think about why this is true before reading the solution.

1. Suppose x and y are integers such that $5x + 8y = 120$. Rearranging $5x + 8y = 120$, we have that $5x = 120 - 8y$, and after factoring 8 out of the right side, we get $5x = 8(15 - y)$. This means $5x$ is a multiple of 8. Using the fact given before the solution and the fact that $\gcd(5, 8) = 1$, we get that x is a multiple of 8. Similarly, $8y = 120 - 5x = 5(24 - x)$, so y is a multiple of 5.

   Now suppose x and y are non-negative integers such that $5x + 8y = 120$. By the previous paragraph, there are integers $X \geq 0$ and $Y \geq 0$ such that $x = 8X$ and $y = 5Y$, which means $5(8X) + 8(5Y) = 120$. Dividing by 40, we get $X + Y = 3$. Since X and Y are non-negative integers, (X, Y) must be one of the four pairs $(0, 3)$, $(1, 2)$, $(2, 1)$, and $(3, 0)$.

   Since $x = 8X$ and $y = 5Y$, this means the only possible non-negative solutions are

   $$\begin{array}{llll} x = 0 & x = 8 & x = 16 & x = 24 \\ y = 15 & y = 10 & y = 5 & y = 0 \end{array}$$

   It is easy to check that each of these pairs is indeed a non-negative solution to $5x+8y = 120$.

2. Observe the following:

   $$\begin{aligned} 5(4) + 8(1) &= 28 \\ 5(1) + 8(3) &= 29 \\ 5(6) + 8(0) &= 30 \\ 5(3) + 8(2) &= 31 \\ 5(0) + 8(4) &= 32 \end{aligned}$$

   which shows that $5x + 8y = c$ has a non-negative solution when $c = 28$, $c = 29$, $c = 30$, $c = 31$, and $c = 32$.

   Next, observe that if $5x + 8y = c$ has a non-negative solution $(x, y) = (u, v)$, then

   $$\begin{aligned} 5(u + 1) + 8v &= 5u + 8v + 5 \\ &= c + 5, \end{aligned}$$

   so $5x+8y = c+5$ has a non-negative solution, namely $(x, y) = (u+1, v)$. Since $5x+8y = 28$ has a non-negative solution, so does $5x + 8y = 28 + 5 = 33$. Since $5x + 8y = 29$ has a non-negative solution, so does $5x + 8y = 29 + 5 = 34$. Continuing in this way, we get that $5x + 8y = c$ has a non-negative solution for $c = 33$, $c = 34$, $c = 35$, $c = 36$, and

$c = 37$. This process can be repeated to get that $5x + 8y = c$ has a non-negative solution for all $c \geq 28$. It was important that we started with five consecutive values of c for which $5x + 8y = c$ has a non-negative solution.

To finish the solution to this part, we will argue that $5x + 8y = 27$ has no non-negative solution. Together with the fact that $5x + 8y = c$ has a non-negative solution for every $c \geq 28$, this will show that the answer to the question is $c = 27$.

Suppose $5x+8y = 27$ for non-negative integers x and y. Rearranging, we have $8y = 27-5x$. Since x is a non-negative integer, $27-5x$ has a units digit of either 7 or 2. However, $27-5x$ must be a non-negative multiple of 8 since it is equal to $8y$. There are no multiples of 8 with a units digit of 7, and the smallest nonnegative multiple of 8 with a units digit of 2 is 32. Therefore, $27 - 5x$ cannot be a non-negative multiple of 8 if x is a non-negative integer, so there are no non-negative solutions to $5x + 8y = 27$.

Before moving on to the solutions to Questions 3, 4, and 5, we will state two facts that will come up in their solutions. The proofs of these facts can be found at the end of this document.

Fact 1: Suppose a and b are positive integers with $\gcd(a, b) = 1$. For every integer c, the equation $ax + by = c$ has an integer solution.

Fact 2: Suppose a and b are positive integers with $\gcd(a, b) = 1$, that c is an integer, and that $(x, y) = (u, v)$ is an integer solution to $ax + by = c$ (which must exist by Fact 1). For every integer k, the pair $(u + bk, v - ak)$ is a solution to $ax + by = c$. In addition, this gives every integer solution to $ax + by = c$.

Fact 2 says that finding all integer solutions to $ax + by = c$ comes down to finding one integer solution.

3. In Question 2, we saw that when $a = 5$ and $b = 8$, the answer is $c = 27$. It may take some experimentation to guess a pattern. For example, if $a = 4$ and $b = 3$, you will find that $c = 5$ is the smallest positive integer for which $ax + by = c$ has no non-negative solution. For another example, if $a = 6$ and $b = 7$, then $c = 29$ is the largest positive integer for which $ax + by = c$ has no non-negative solution. Even now, it might be tricky to notice a pattern. If 1 is added to each of these largest values of c, one gets 28 for $a = 5$ and $b = 8$, 6 for $a = 4$ and $b = 3$, and 30 for $a = 6$ and $b = 7$. These integers factor as $28 = 4 \times 7$, $6 = 3 \times 2$, and $30 = 5 \times 6$. With such an observation, you might guess that the largest integer c for which there are no non-negative solutions to $ax + by = c$ is $(a - 1)(b - 1) - 1 = ab - a - b$. This would be a correct guess, and we will now prove it!

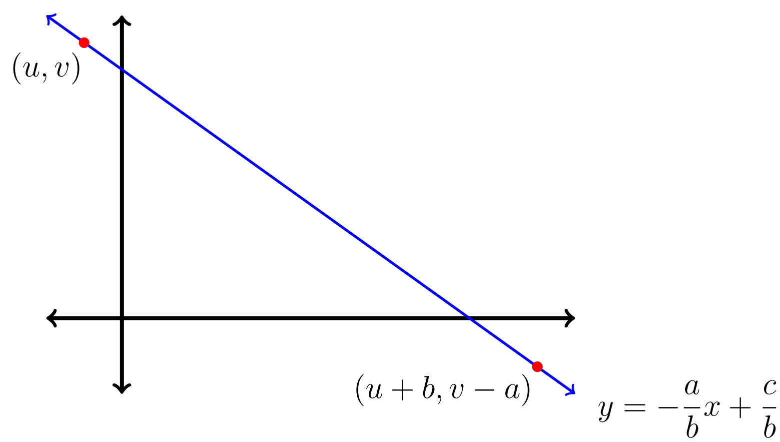
   We will prove two statements.

   - If a and b are positive integers with $\gcd(a, b) = 1$ and $ax+by = c$ has no non-negative solution, then $c \leq ab - a - b$.
   - If a and b are positive integers with $\gcd(a, b) = 1$, then $ax + by = ab - a - b$ has no non-negative solution.

   The first bullet point implies that if $c > ab - a - b$, then $ax + by = c$ *does* have a non-negative solution. Therefore, the two statements above combine to imply that the answer to the question is $c = ab - a - b$.

Assume that c is a positive integer such that $ax+by=c$ has no non-negative solution. We can rearrange $ax+by=c$ to $y=-\frac{a}{b}x+\frac{c}{b}$. This is the equation of a line with negative slope and a positive y-intercept. Furthermore, the solutions to $ax+by=c$ are exactly the *lattice points* that lie on the line [A lattice point is a point in the plane whose coordinates are both integers.]. By Fact 2, the integer solutions to $ax+by=c$, which are the lattice points on the line, are exactly the ordered pairs of the form $(u+bk, v-ak)$ where $(x,y)=(u,v)$ is any fixed integer solution and k takes every integer value. This means there are infinitely many lattice points on the line and that their x-coordinates occur at $x=u$ and every integer multiple of b to the right and left of u. Likewise, their y-coordinates occur at v and every integer multiple of a above and below v.

Thus, there must be a solution $(x,y)=(u,v)$ with the property that $u<0$ but $u+b\geq 0$. We will fix the solution $(x,y)=(u,v)$ to be the lattice point on the line $y=-\frac{a}{b}x+\frac{c}{b}$ that is closest to the y-axis among those with a negative x-coordinate. Since $u<0$ and u is an integer, it must be that $u\leq -1$. The diagram below depicts the line $y=-\frac{a}{b}x+\frac{c}{b}$ as well as the lattice point (u,v), and the next lattice point on the line moving from (u,v) to the right. We are assuming there are no non-negative solutions, which means the next lattice point cannot be in the first quadrant. However, it has a positive x-coordinate by the assumption on (u,v), so it must appear below the x-axis in order to fail to be a non-negative solution.



The next lattice point on the line moving to the right from (u,v) is $(u+b, v-a)$. As mentioned above, it must be in the fourth quadrant, which means $v-a<0$. Since v and a are both integers, so is $v-a$, which means $v-a\leq -1$ which can be rearranged to $v\leq a-1$.

We now have that $au+bv=c$ as well as $u\leq -1$ and $v\leq a-1$. Therefore,

$$\begin{aligned} c &= au+bv \\ &\leq a(-1)+b(a-1) \\ &= ab-a-b. \end{aligned}$$

Therefore, if $ax+by=c$ has no non-negative solutions, then $c\leq ab-a-b$, as claimed.

For the second statement, suppose $ax+by=ab-a-b$ for integers x and y. Rearranging and factoring, we get $a(x+1)+b(y+1)=ab$. Since both $a(x+1)$ and ab are multiples of a, it must also be the case that $b(y+1)$ is a multiple of a. We are assuming that $\gcd(a,b)=1$, so this means $y+1$ is a multiple of a. Therefore, there is some integer Y so that $y+1=aY$. By similar reasoning, there is an integer X such that $x+1=bX$.

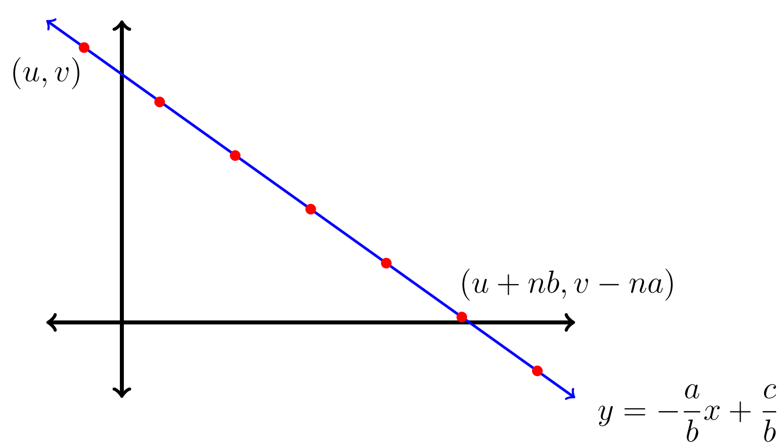
Substituting $y+1=aY$ and $x+1=bX$ into $a(x+1)+b(y+1)=ab$, we get the equation $abX+abY=ab$, and since ab must be positive, we can divide through by it to get $X+Y=1$. If the sum of two integers is 1, then one of them must be non-positive. Therefore, either $X\leq 0$ or $Y\leq 0$. By how X and Y are defined, this means either $\dfrac{x+1}{b}\leq 0$ or $\dfrac{y+1}{a}\leq 0$. Since a and b are positive, this means either $x+1\leq 0$ or $y+1\leq 0$, which implies that one of x and y is negative. Therefore, no integer solution to $ax+by=ab-a-b$ can be non-negative.

As discussed earlier, we have shown that $ax+by=c$ has a non-negative solution for every integer $c>ab-a-b$ and we have now shown that $ax+by=ab-a-b$ has no non-negative solution. Therefore, $c=ab-a-b$ is the largest integer with the property that $ax+by=c$ has no non-negative solution.

4. We will show that for every positive integer n, there are exactly ab positive integers c for which there are exactly n non-negative solutions to $ax+by=c$.

   Suppose c has the property that there are exactly n non-negative solutions to $ax+by=c$. Following the reasoning in the solution to 3., we are interested in lattice points on the line $y=-\frac{a}{b}x+\frac{c}{b}$. As discussed earlier, there are infinitely many such lattice points and we can choose (u,v) to be the lattice point on the line with the property that $u<0$ and $u+b\geq 0$. The next n lattice points on the line moving to the right are those of the form $(u+kb,v-ka)$ where k ranges over the integers from 1 through n inclusive.

   In order for there to be exactly n non-negative solutions, the first n lattice points on the line to the right of (u,v) must be in the first quadrant. The diagram below is similar to the one in the solution to Question 3, but it depicts the situation for $n=5$. The point (u,v) is in the second quadrant, the next five moving along the line to the right are in the first quadrant, and the next lattice point, $(u+(n+1)b,v-(n+1)a)$, is in the fourth quadrant.



   For $(u+(n+1)b,v-(n+1)a)$ to be the first lattice point on the line to the right of (u,v) that does not correspond to a non-negative solution, it must not be in the first quadrant while $(u+nb,v-na)$ must be in the first quadrant. Since k and b are positive, the assumptions on (u,v) imply that $(u+kb, v-ka)$ has a non-negative x-coordinate for *every* positive integer k. This means $(u+nv, v-na)$ has a non-negative y-coordinate and $(u+(n+1)b, v-(n+1)a)$ has a negative y-coordinate. This leads to the two inequalities $v-na \geq 0$ and $v-(n+1)a < 0$.

From our assumption about c, we have deduced that there is a nonnegative solution (u,v) satisfying u and v satisfying $u < 0$, $u+b \geq 0$, $v-na \geq 0$, and $v-(n+1)a < 0$. Since all quantities are integers, we can replace the inequality $u < 0$ with $u \leq -1$ and replace $v-(n+1)a < 0$ with $v-(n+1)a \leq -1$. Rearranging and combining these inequalities, we have

$$-b \leq u \leq -1 \tag{1}$$

$$na \leq v \leq (n+1)a - 1 \tag{2}$$

There are b integers u satisfying (1) and there are a integers v satisfying (2). We now have that if c is such that there are exactly n non-negative solutions to $ax+by=c$, then there are integers u and v satisfying (1) and (2) respectively, as well as $au+bv=c$.

Next, we suppose u satisfies (1) and v satisfies (2) and define $c = au+bv$. The inequalities (1) and (2) imply $u < 0$, $u+b \geq 0$, $v-na \geq 0$, and $v-(n+1)a < 0$. Following the reasoning from earlier in this part and in the solution to 3, this means $ax+by=c$ has exactly n non-negative solutions. Moreover, since $n \geq 1$, we have

$$c = au+bv \geq a(-b)+b(na) \geq -ab+ab = 0$$

which says that c is non-negative. [It is worth remarking here that if $n=0$, there are still are exactly ab integers c for which there are n non-negative solutions to $ax+by=c$. However, some of those integers will be negative. With $n \geq 1$, all of the integers c for which there are exactly n non-negative solutions to $ax+by=c$ happen to be non-negative.]

We have that $ax+by=c$ has exactly n non-negative solutions exactly when c takes the form $c = au+bv$ for some integers u satisfying (1) and v satisfying (2). Since there are b choices for an integer u satisfying (1) and a choices for an integer v satisfying (2), there are at most ab values of c that satisfy these conditions. To finish the argument, we must show that we indeed get ab distinct integers when computing $au+bv$ for every possible choice of u satisfying (1) and v satisfying (2).

To do this, we will assume that u_1 and u_2 both satisfy (1), that v_1 and v_2 both satisfy (2), and that $au_1+bv_1 = au_2+bv_2$ and deduce that $u_1=u_2$ and $v_1=v_2$. By possibly relabelling, we can assume that $u_1 \geq u_2$. With these assumptions, rearrange $au_1+bv_1 = au_2+bv_2$ to get $a(u_1-u_2) = b(v_2-v_1)$. This means $a(u_1-u_2)$ is a multiple of b. Since $\gcd(a,b)=1$, u_1-u_2 is a multiple of b. However, both u_1 and u_2 are between $-b$ and -1 inclusive, so their difference is smaller than b. We have that $0 \leq u_1-u_2 < b$ is a multiple of b. The only possibility is that $u_1-u_2=0$, or $u_1=u_2$. This means $b(v_1-v_2)=0$ as well, and since $b \neq 0$, $v_1=v_2$.

The question asked for the answer with $n=2025$, but we have shown that the answer is ab for every integer $n \geq 1$, which includes $n=2025$.

5. From the reasoning in 4., we know that the positive integers c with the property that $ax+by=c$ has exactly n non-negative solutions are exactly the integers of the form $au+bv=c$ where $-b \leq u \leq -1$ and $na \leq v \leq (n+1)a-1$.

Observe that there are exactly b possible values of u and a possible values of v, so we need to add ab integers together.

We will do this by examining the u's first, then the v's. Observe that the sum contains exactly a copies of au for every u satisfying $-b \leq u \leq -1$. Therefore, the "u part" of the sum is

$$\begin{aligned}
&a(-a - 2a - 3a - 4a - \cdots - (b-1)a - ba) \\
&= -a^2(1 + 2 + 3 + \cdots + (b-1) + b) \\
&= -\frac{a^2b(b+1)}{2}.
\end{aligned}$$

By similar reasoning, the sum contains exactly b copies of the term bv for every v satisfying $na \leq v \leq (n+1)a - 1 = na + a - 1$. This means the "$v$ part" of the sum is

$$\begin{aligned}
&b\big(bna + b(na+1) + b(na+2) + \cdots + b(na+a-2) + b(na+a-1)\big) \\
&= b^2\big(na + (na+1) + (na+2) + \cdots + (na+a-2) + (na+a-1)\big) \\
&= b^2\big(a(na) + 1 + 2 + 3 + \cdots + (a-2) + (a-1)\big) \\
&= a^2b^2n + b^2(1 + 2 + 3 + \cdots + (a-2) + (a-1)) \\
&= a^2b^2n + \frac{b^2(a-1)a}{2}
\end{aligned}$$

Therefore, the sum we seek is

$$\begin{aligned}
a^2b^2n + \frac{b^2(a-1)a}{2} - \frac{a^2b(b+1)}{2} &= \frac{ab}{2}\left(2abn + b(a-1) - a(b+1)\right) \\
&= \frac{ab}{2}\left(2abn + ab - b - ab - a\right) \\
&= \frac{ab}{2}\left(2abn - a - b\right).
\end{aligned}$$

As promised, we now include proofs of Fact 1 and Fact 2, which were stated between the solutions to Questions 2 and 3. The proof of Fact 1 makes use of the fact that if $\gcd(a,b) = 1$, then $ax + by = 1$ always has an integer solution. This is a well known fact from number theory that you may wish to look up.

Fact 1: Suppose a and b are positive integers with $\gcd(a,b) = 1$. For every integer c, the equation $ax + by = c$ has an integer solution.

Proof. There are integers u' and v' such that $au' + bv' = 1$ (see above). Setting $u = cu'$ and $v = cv'$, we have $au + bv = acu' + bcv' = c(au' + bv') = c(1) = c$. $\square$

Fact 2: Suppose a and b are positive integers with $\gcd(a,b) = 1$, that c is an integer, and that $(x,y) = (u,v)$ is an integer solution to $ax + by = c$ (which must exist by Fact 1). For every integer k, the pair $(u + bk, v - ak)$ is a solution to $ax + by = c$. In addition, this gives every integer solution to $ax + by = c$.

Proof. To see that $(u + bk, v - ak)$ is a solution, we can substitute and simplify:

$$\begin{aligned} a(u + bk) + b(v - ak) &= au + abk + bv - abk \\ &= au + bv \\ &= c \end{aligned}$$

since $(x, y) = (u, v)$ is a solution to $ax + by = c$ by assumption.

To see that every solution takes the form $(u + bk, v - ak)$ is slightly trickier and requires use of the fact that $\gcd(a, b) = 1$.

Suppose $(x, y) = (u', v')$ is also a solution to $ax + by = c$. This means $au' + bv' = c$. We also have that $au + bv = c$, so we can subtract to get

$$(au + bv) - (au' + bv') = c - c = 0$$

which can be rearranged and factored to get $a(u' - u) = b(v - v')$.

In the equation above, a, b, $u' - u$, and $v - v'$ are all integers, and so we have that $a(u' - u)$ is a multiple of b. Since $\gcd(a, b) = 1$, $u' - u$ is a multiple of b, which means there is some integer k such that $u' - u = bk$. Substituting this into $a(u' - u) = b(v - v')$ gives $abk = b(v - v')$, and after cancelling b from both sides, we have $v - v' = ak$.

Rearranging $u' - u = bk$ and $v - v' = ak$ to $u' = u + bk$ and $v' = v - ak$ shows that the solution $(x, y) = (u', v')$ takes the form $(u + bk, v - ak)$, as claimed. $\square$

Problem of the Month

Problem 1: Displacing Permutations

October 2025

In this problem, X_n will denote the set of integers $\{1, 2, 3, \ldots, n\}$. A *permutation* of X_n is an ordered list of these integers that contains each of them exactly once. For example, there are exactly 6 permutations of X_3, and they are

123 132 213 231 312 321

Another way to think about a permutation is as a function from the set X_n to itself, where no two inputs to the function have the same output. For example, the permutation 213 of X_3 represents the function that sends 1 to 2, sends 2 to 1, and sends 3 to itself. The permutation σ of X_5 denoted by 43512 satisfies $\sigma(1) = 4$, $\sigma(2) = 3$, $\sigma(3) = 5$, $\sigma(4) = 1$, and $\sigma(5) = 2$.

In this problem, the *displacement* of a permutation σ of X_n is equal to $\mathbf{D}(\sigma) = \sum_{i=1}^{n} |i - \sigma(i)|$. For example, with σ from the paragraph above, we have

$$\begin{aligned}\mathbf{D}(\sigma) &= |1 - \sigma(1)| + |2 - \sigma(2)| + |3 - \sigma(3)| + |4 - \sigma(4)| + |5 - \sigma(5)| \\ &= |1 - 4| + |2 - 3| + |3 - 5| + |4 - 1| + |5 - 2| \\ &= 3 + 1 + 2 + 3 + 3 = 12\end{aligned}$$

1. Suppose $n \geq 2$. Determine the number of permutations σ of X_n that satisfy $\mathbf{D}(\sigma) = 2$.
2. Suppose $n \geq 4$. Determine the number of permutations σ of X_n that satisfy $\mathbf{D}(\sigma) = 4$.
3. Prove for all $n \geq 2$, if σ is a permutation of X_n, then $\mathbf{D}(\sigma)$ is even.
4. Given an odd positive integer n and a permutation σ of X_n, determine the maximum possible value of $\mathbf{D}(\sigma)$.
5. Given an odd positive integer n, determine the number of permutations σ of X_n have the property that $\mathbf{D}(\sigma)$ is equal to the maximum from the previous question.

Problem of the Month

Problem 1: Displacing Permutations

October 2025

Hint

1. Explicitly compute $\mathbf{D}(\sigma)$ for all permutations in X_3. Then try it for X_4. What do you notice about the permutations satisfying $\mathbf{D}(\sigma) = 2$?

2. See if you can argue that at most four integers in $\{1, 2, 3, \ldots, n\}$ can satisfy $\sigma(i) \neq i$. How must those integers interact with each other?

3. It may be helpful here to consider the path a single integer takes under repeated application of the permutation. For example, in the permutation σ denoted by 58123764, we can start with 1 and repeatedly apply the permutation. We get, $\sigma(1) = 5$, $\sigma(5) = 3$, $\sigma(3) = 1$, and then the pattern repeats. We can denote this by $1 \to 5 \to 3 \to 1$. Similarly, the path 2 takes is $2 \to 8 \to 4 \to 2$.

4., 5. For a permutation σ in X_{2k+1}, think about how a σ that maximizes $\mathbf{D}(\sigma)$ must behave on the following three sets: $\{1, 2, \ldots, k\}, \{k + 1\}, \{k + 2, \ldots, 2k, 2k + 1\}$.

Problem of the Month

Solution to Problem 1: Displacing Permutations

October 2025

1. The quantity $\mathbf{D}(\sigma)$ is a sum of absolute values of the form $|\sigma(i) - i|$ where $\sigma(i)$ and i are both integers. Therefore, each term in the sum defining $\mathbf{D}(\sigma)$ is a non-negative integer. The only way to have a sum of non-negative integers equal to 2 is for one integer to be 2 and rest 0, or for two of them to be equal to 1 and the rest equal to 0.

   If the quantity $|\sigma(i) - i| = 0$, then $\sigma(i) = i$. If σ satisfies $\sigma(i) = i$ for $n-1$ values of i from 1 through n, then it must satisfy $\sigma(i) = i$ for *all* values of i from 1 through n. This because permutations are functions that send each input to a different output. Thus, if $\sigma(i) = i$ for $n-1$ values of i, then there is only one place for the nth value to be sent by σ, and that value is itself.

   Therefore, having $|\sigma(i) - i| = 2$ for one value of i and all others equal to 0 is not possible. Thus, if $\mathbf{D}(\sigma) = 2$, then there must be exactly two integers i between 1 and n inclusive such that $|\sigma(i) - i| = 1$.

   Suppose a is the smallest integer that satisfies $|\sigma(a) - a| = 1$. Then $\sigma(a) = a - 1$ or $\sigma(a) = a + 1$. If $\sigma(a) = a - 1$, then it is impossible for $\sigma(a-1) = a-1$ (since a permutation cannot send two inputs to the same output) contradicting our assumption that a is the smallest integer not sent to itself. Thus, we must have $\sigma(a) = a+1$. We also have that $\sigma(a+1) \neq a+1$ for the same reasoning as above. If $\sigma(a+1) \neq a$, then there must be some third integer that is not fixed by σ. Thus, we have $\sigma(a+1) = a$.

   We conclude that if $\mathbf{D}(\sigma) = 2$, then σ interchanges two adjacent integers and fixes all others. For example, $\sigma(1) = 2$ and $\sigma(2) = 1$, and $\sigma(i) = i$ for all $i \geq 3$ is such a permutation.

   There are $n-1$ such permutations, so the answer to the question is $n-1$.

2. By similar reasoning to that which was used in the previous solution, if $\mathbf{D}(\sigma) = 4$, then 4 is a sum of non-negative integers, which means "most" of the integers must be 0. Again, it is impossible for a permutation to have exactly one point that is not fixed, so the sum being composed of 4 and $(n-1)$ zeros is not possible.

   The other possibilities are $1+3$, $2+2$, $1+1+2$, and $1+1+1+1$ (and all other integers equal to 0). The sum $1+3$ is not possible since if $|\sigma(i) - i| = 1$, then $\sigma(i) = i \pm 1$, which means $i \pm 1$ is not fixed. If $i-1$ is not fixed, then we must have $|\sigma(i-1) - (i-1)| = 3$, and so $\sigma(i-1) = i-4$ or $\sigma(i-1) = i+2$. Then either $i-4$ or $i+2$ would not be fixed, which means the sum defining $\mathbf{D}(\sigma)$ would have at least three nonzero summands, which is contrary to our assumption.

   The other sums, $2+2$, $1+1+2$, and $1+1+1+1$ are all possible.

   If the sum is $2+2$, then there are two integers that are not fixed, and each is moved to a position 2 away from it. The only way to do this is to exchange two integers that differ by 2. There are $n-2$ such permutations.

The only way to achieve the sum $1+1+2$ is by "cycling" three adjacent integers. That is, there is some integer i such that $\sigma(i) = i+1$, $\sigma(i+1) = i+2$, and $\sigma(i+2) = i$ *or* $\sigma(i) = i-1$, $\sigma(i-1) = i-2$, and $\sigma(i-2) = i$. This can be shown using the same kind of reasoning that has already been used. There are $2 \times (n-2)$ such permutations.

For $\mathbf{D}(\sigma)$ to occur as $1+1+1+1$ plus $(n-4)$ zeros, there must be two pairs, a and b, with $b - a \geq 2$ such that $\sigma(a) = a+1$, $\sigma(a+1) = a$, $\sigma(b) = b+1$, and $\sigma(b+1) = b$.

If $a = 1$, then b can be any of $3, 4, 5, \ldots, n-1$, for a total of $n-3$ choices for b. if $a = 2$, then there are $n-4$ choices for b. If $a = 3$, then there are $n-5$ choices for b. The largest possible value of a is $n-3$, and in this case we must have $b = n-1$, so there is 1 possibility.

There are $1 + 2 + 3 + \cdots + (n-3) = \dfrac{(n-3)(n-2)}{2}$ permutations in this case.

Therefore, the total number of permutations with $\mathbf{D}(\sigma) = 4$ is

$$3(n-2) + \frac{(n-3)(n-2)}{2} = \frac{(n-2)(6+n-3)}{2} = \frac{(n-2)(n+3)}{2}$$

3. First, we will address the question for permutations that are *cycles*. An example of a cycle is permutation 462351 since $\sigma(1) = 4$, $\sigma(4) = 3$, $\sigma(3) = 2$, $\sigma(2) = 6$, and $\sigma(6) = 1$. Note that $\sigma(5) = 5$, so the permutation "cycles" 1 to 4 to 3 to 2 to 6 and back to 1, and fixes every other integer, which is 5. We can express this cycle as

$$1 \to 4 \to 3 \to 2 \to 6 \to 1$$

As another example, the permutation

$$5 \to 1 \to 7 \to 2 \to 4 \to 5$$

of X_7 is equal to the permutation 7435162. In this permutation, we have $\sigma(5) = 1$, $\sigma(1) = 7$, $\sigma(7) = 2$, $\sigma(2) = 4$, and $\sigma(4) = 5$, as well as $\sigma(3) = 3$, and $\sigma(6) = 6$. This means $|\sigma(3) - 3| = |\sigma(6) - 6| = 0$, and the other summands in $\mathbf{D}(\sigma)$ are

$$\begin{aligned}
|\sigma(5) - 5| &= 4 \\
|\sigma(1) - 1| &= 6 \\
|\sigma(7) - 7| &= 5 \\
|\sigma(2) - 2| &= 2 \\
|\sigma(4) - 4| &= 1
\end{aligned}$$

Therefore, $\mathbf{D}(\sigma) = 0 + 0 + 4 + 6 + 5 + 2 + 1 = 18$, which is indeed even. The important thing to take away here is that the number of odd numbers in the sum is 2 (and of course, 2 is even!).

Suppose a cycle σ on X_n has the form

$$a_1 \to a_2 \to a_3 \to \cdots \to a_k \to a_1$$

which implies that k elements are moved by σ, and the other $n-k$ are not. Then we have $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, and so on up to $\sigma(a_{k-1}) = a_k$ and then $\sigma(a_k) = a_1$. We then have

$$\begin{aligned}
\mathbf{D}(\sigma) &= |\sigma(a_1) - a_1| + |\sigma(a_2) - a_2| + |\sigma(a_3) - a_3| + \cdots + |\sigma(a_{k-1}) - a_{k-1}| + |\sigma(a_k) - a_k| \\
&= |a_2 - a_1| + |a_3 - a_2| + |a_4 - a_3| + \cdots + |a_k - a_{k-1}| + |a_1 - a_k|
\end{aligned}$$

Each term of the form $|a_i - a_j|$ is even if a_i and a_j have the same parity, and it is odd if they have different parity. Thus, the number of odd terms in the sum above is equal to the number of times that the list

$$a_1, a_2, a_3, \ldots, a_{k-1}, a_1$$

changes parity. However, the list above has the same first and last number, so the parity must eventually change back to its original parity. In other words, the parity must change an even number of times, so there are an even number of odd integers in the sum above.

The sum of a list of integers, an even number of which are odd, must be an even number.

This shows that if σ is a cycle, then $\mathbf{D}(\sigma)$ is even. We now note that every permutation is composed of several cycles. For example, the permutation 58123764 satisfies

$$\begin{aligned} 1 &\to 5 \\ 2 &\to 8 \\ 3 &\to 1 \\ 4 &\to 2 \\ 5 &\to 3 \\ 6 &\to 7 \\ 7 &\to 6 \\ 8 &\to 4 \end{aligned}$$

So we have $1 \to 5 \to 3 \to 1$, and this gives all of the information about what σ does to 1, 3, and 5. We can then start with 2 to get $2 \to 8 \to 4 \to 2$, and then $6 \to 7 \to 6$. Thus, σ breaks into two cycles consisting of three distinct integers, and one cycle consisting of two distinct integers. The sum defining $\mathbf{D}(\sigma)$ can likewise be decomposed into

$$\Big(|\sigma(1)-1|+|\sigma(5)-5|+|\sigma(3)-3|\Big)+\Big(|\sigma(2)-2|+|\sigma(8)-8|+|\sigma(4)-4|\Big)+\Big(|\sigma(6)-6|+|\sigma(7)-7|\Big)$$

which is a sum of three even numbers.

4. Suppose $n = 2k + 1$ for some positive integer k and that σ is a permutation of X_n. We will show that the maximum value of $\mathbf{D}(\sigma)$ is attained for any permutation satisfying

   - if $i < k + 1$, then $\sigma(i) \geq k + 1$, and
   - if $i > k + 1$, then $\sigma(i) \leq k + 1$.

   For example, when $n = 5$, such a permutation must send each of 1 and 2 to $3, 4$, or 5, and it must send each of 4 and 5 to 1, 2, or 3. Roughly, the kinds of permutations we're after send the first half of the list to the second half, and the send half to the first half (of course, there are an odd number of integers in the list, so first and second half isn't precisely correct here).

   Suppose there is some $a \leq k$ such that $\sigma(a) \leq k$. The existence of such an a implies that there is some $c \geq k+2$ such that $\sigma(c) \geq k+2$. Otherwise, each of the $(2k+1)-(k+1) = k$ integers that are at least $k + 2$, as well as a, are all sent by σ to the integers $1, 2, \ldots, k$. This would imply that at least two of $a, k + 2, k + 3, \ldots, 2k + 1$ are sent to the same value by σ, but this is impossible since σ is a permutation.

Thus, if there is some $a \leq k$ with $\sigma(a) \leq k$, then there is some $c \geq k+2$ such that $\sigma(c) \geq k+2$. Assume that $a \leq k$, $b \leq k$, $c \geq k+2$, and $d \geq k+2$ satisfy $\sigma(a) = b$ and $\sigma(c) = d$. It is possible that $a = b$ or $c = d$ or both.

Let τ be the permutation given by

$$\tau(a) = d, \quad \tau(c) = b \quad \text{and} \quad \tau(i) = \sigma(i)$$

if $i \neq a$ and $i \neq c$. This is still a permutation. The terms in $\mathbf{D}(\sigma)$ and $\mathbf{D}(\tau)$ are identical except that the terms $|a-b|$ and $|c-d|$ from the displacement of σ are replaced by $|a-d|$ and $|c-b|$ respectively in the displacement of τ. In other words,

$$\mathbf{D}(\tau) - \mathbf{D}(\sigma) = |d-a| + |b-c| - |b-a| - |d-c|.$$

Note that a and b are at most k and c and d are at least $k+2$, so we know that $a < c$, $a < d$, $b < c$, and $b < d$. We will consider four possible cases for how a and b compare, and how c and d compare.

<u>$a \leq b$ and $c \leq d$</u>: Then

$$\begin{aligned} |d-a| + |b-c| - |b-a| - |d-c| &= (d-a) + (c-b) - (b-a) - (d-c) \\ &= 2c - 2b > 0 \end{aligned}$$

<u>$a \leq b$ and $c > d$</u>: Then

$$\begin{aligned} |d-a| + |b-c| - |b-a| - |d-c| &= (d-a) + (c-b) - (b-a) - (c-d) \\ &= 2d - 2b > 0 \end{aligned}$$

<u>$a > b$ and $c \leq d$</u>: Then

$$\begin{aligned} |d-a| + |b-c| - |b-a| - |d-c| &= (d-a) + (c-b) - (a-b) - (d-c) \\ &= 2c - 2a > 0 \end{aligned}$$

<u>$a > b$ and $c > d$</u>: Then

$$\begin{aligned} |d-a| + |b-c| - |b-a| - |d-c| &= (d-a) + (c-b) - (a-b) - (c-d) \\ &= 2d - 2a > 0 \end{aligned}$$

No matter which of the four possibilities are true (and one of them must be true), we get that $\mathbf{D}(\tau) - \mathbf{D}(\sigma) > 0$, or $\mathbf{D}(\tau) > \mathbf{D}(\sigma)$.

So, what have we shown with all of these calculations? Recall the two properties from the beginning of the solution to this question:

(1) If $i < k+1$, then $\sigma(i) \geq k+1$.

(2) If $i > k+1$, then $\sigma(i) \leq k+1$.

We have shown that if σ does not satisfy Property (1), then there is a permutation τ with $\mathbf{D}(\sigma) < \mathbf{D}(\tau)$. Similarly, you can show that if σ does not satisfy Property (2), then there is a permutation τ with $\mathbf{D}(\sigma) < \mathbf{D}(\tau)$ (see if you can do this!).

Therefore, a permutation σ that maximizes $\mathbf{D}(\sigma)$ must satisfy both Properties (1) and (2).

We will now show that $\mathbf{D}(\sigma)$ is constant for all such permutations. To see this, suppose σ is a permutation with the property from the previous paragraph. Suppose a and b are less than k, and that $\sigma(a) = c$ and $\sigma(b) = d$. From our assumption, we must have $c \geq k+1$ and $d \geq k+1$. Let τ be the permutation with $\tau(a) = d$, $\tau(b) = c$, and $\tau(i) = \sigma(i)$ for all other i. By very similar reasoning that which was used earlier,

$$\mathbf{D}(\tau) - \mathbf{D}(\sigma) = |d-a| + |c-b| - |c-a| - |d-b|$$

Since we know that $a \leq c$, $a \leq d$, $b \leq c$, and $b \leq d$, we have

$$\mathbf{D}(\tau) - \mathbf{D}(\sigma) = |d-a| + |c-b| - |c-a| - |d-b| = (d-a) + (c-b) - (c-a) - (d-b) = 0$$

Similarly, if we exchange the images under σ of two integers that are at least $k+2$, the displacement will not change.

We leave it to the reader to convince themself that every permutation of X_n can be attained from every other permutation by a sequence of such interchanges (*Hint:* Swap the values of $\sigma(a)$ and $\sigma(b)$ for some a and b, and leave everything else alone). Thus, we only need to compute $\mathbf{D}(\sigma)$ for one permutation σ with the property that $\sigma(i) \geq k+1$ when $i \leq k$ and $\sigma(i) \geq k+1$ when $i \geq k+2$. One such permutation is as follows: $\sigma(k+1) = k+1$, $\sigma(i) = i+k+1$ for $i \leq k$, and $\sigma(i) = i-k-1$ for $i \geq k+2$. Note that $|\sigma(k+1)-(k+1)| = 0$, while $|\sigma(i) - i| = k+1$ for all other i. Thus,

$$\mathbf{D}(\sigma) = 0 + 2k(k+1) = (n-1)\left(\frac{n-1}{2} + 1\right) = \frac{n^2-1}{2}$$

5. In the previous problem, we shows that $\mathbf{D}(\sigma)$ is maximized precisely when σ satisfies
   - if $i < k+1$, then $\sigma(i) \geq k+1$, and
   - if $i > k+1$, then $\sigma(i) \leq k+1$.

   To count how many permutations satisfy the two conditions above, we will first choose the value of $\sigma(k+1)$, and then count the number of permutations that are possible.

   Suppose $\sigma(k+1) = k+1$. Then for each $i < k+1$, $\sigma(i) > k+1$. There are $k!$ ways this can happen. Similarly, there are $k!$ ways $\sigma(j) < k+1$ for $j > k+1$. Therefore, the total number of permutations so that $\mathbf{D}(\sigma)$ is maximized and $\sigma(k+1) = k+1$ is $(k!)^2$.

   Suppose $\sigma(k+1) = t < k+1$ (note that there are k possible values for t). Then for each $j > k+1$, $\sigma(j) \leq k+1$, but $\sigma(j) \neq t$ (since σ is a permutation and t has already been taken by $\sigma(k+1)$). There are $k!$ ways this can happen. For $i < k+1$, we must have $\sigma(i) > k+1$, which contributes another factor of $k!$. Therefore, the total number of permutations so that $\mathbf{D}(\sigma)$ is maximized and $\sigma(k+1) < k+1$ is $k(k!)^2$.

   Finally, if $\sigma(k+1) > k+1$, a similar argument to the previous case gives that the number of possible permutations is $k(k!)^2$.

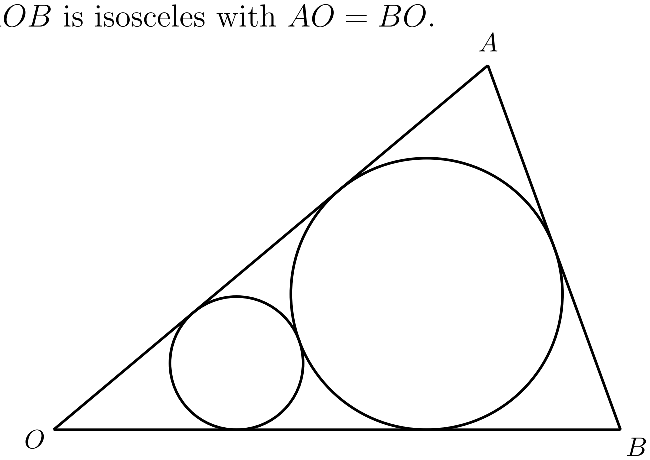
   Putting all of these permutations together, we get an answer of $(2k+1)(k!)^2$.

Problem of the Month

Problem 2: Squeezing circles into a triangle

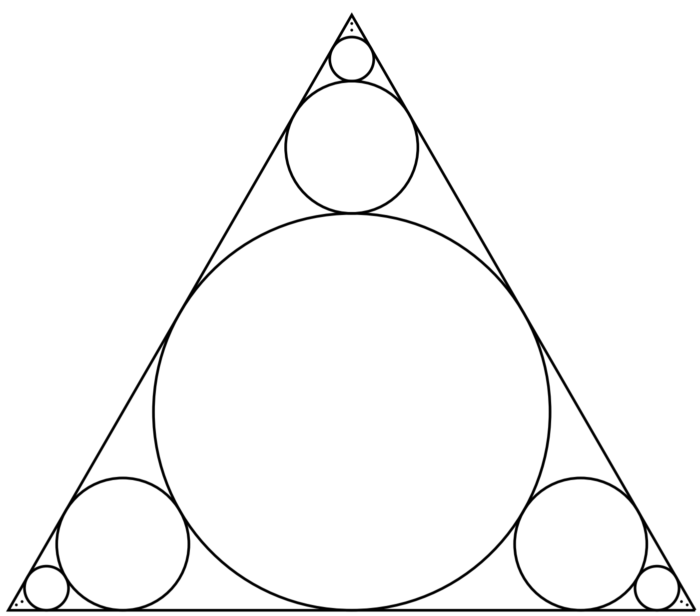
November 2025

1. Let θ be an angle with $0° < \theta < 45°$. In the diagram, points A and B are configured so that $\angle AOB = 2\theta$ and $\triangle AOB$ is isosceles with $AO = BO$.



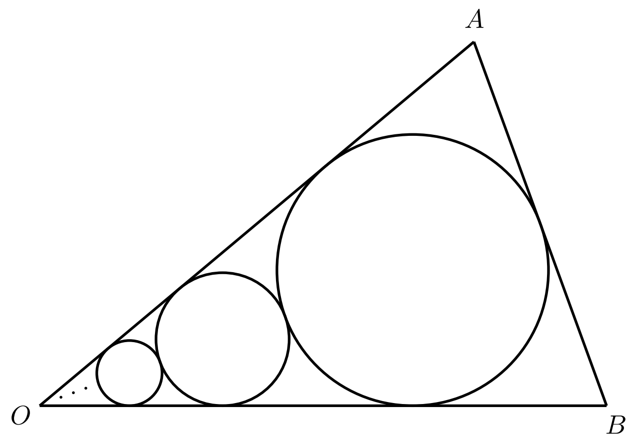
A circle is inscribed in $\triangle AOB$ and another circle is drawn so that it is tangent to the larger circle as well as OA and OB. In terms of θ, find the ratio of the radius of the larger circle to the radius of the smaller circle.

2. Similar to Question 1, an equilateral triangle has a circle inscribed in it. Three circles are then drawn, each tangent to two of the sides of the triangle as well as the larger circle. Another three circles are then drawn, each tangent to two of the three sides of the triangle as well as one of the circles drawn in the previous step.



If this process is continued indefinitely, what fraction of the area of the triangle is covered by circles?

3. Suppose $\triangle AOB$ and θ are as they were defined in Question 1. The process of drawing a circle tangent to OA, OB, and the smallest circle is repeated forever. What fraction of the area of $\triangle AOB$ is covered by circles? Your answer should be in terms of θ.



The result of Question 3 can be applied to solve Question 2. Can you see how?

Problem of the Month

Problem 2: Squeezing circles into a triangle

November 2025

Hint

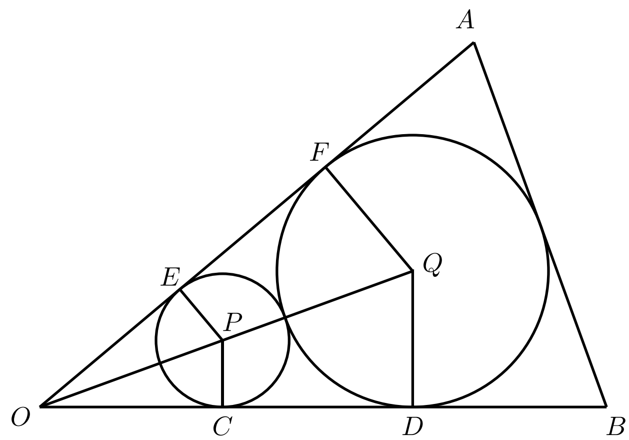
1. There are plenty of ways to approach this problem. One useful construction is to connect the centres of the circles to each other, then draw a perpendicular from each centre to the line OB.
2. It is possible to apply Question 1 with $\theta = 30^\circ$. While there are other ways to do this, the easiest is probably to turn this into a problem of summing an infinite geometric series. You may want to look up how this is done.
3. In some sense, this is a more general version of Question 2. Adding a geometric series will be useful again here, but the terms will be in terms of the arbitrary θ. You might also find it useful to express the area of the triangle and the area of the largest circle in ways that are easy to compare.

Problem of the Month

Solution to Problem 2: Squeezing circles into a triangle

November 2025

1. **Solution 1**: Let P and Q be the centres of the smaller and larger circles, respectively, and let C and D be the points of tangency of the smaller and larger circles to OB. Similarly, let E and F be the points of tangency of the smaller and larger circles to OA.



Line segments PC and PE are radii of the smaller circle and thus are equal. Line segments OE and OC are equal because the distances from two points of tangency to the point where the tangents intersect are equal. We also have that $\angle OEP = \angle OCP = 90°$ because a radius drawn to a point of tangency is perpendicular to that tangent. Therefore, $\triangle OCP$ is congruent to $\triangle OEP$ by side-angle-side congruence. This means $\angle EOP = \angle COP$, so OP is the angle bisector of $\angle EOC = \angle AOB$. By a similar argument, OQ is the angle bisector of $\angle FOD = \angle AOB$. This tells us that P and Q both lie on the angle bisector of $\angle AOB$. Therefore, OPQ is a line segment, and $\angle POC = \dfrac{2\theta}{2} = \theta$.

Let R be the radius of the larger circle and let r be the radius of the smaller circle. It follows from the fact that a radius is perpendicular to the corresponding tangent that line segment PQ passes through the point where the two circles are tangent. This means $PQ = r + R$. Also, since $\dfrac{PC}{OP} = \sin\theta$ and $PC = r$, we get $OP = \dfrac{r}{\sin\theta}$. Therefore, $OQ = \dfrac{r}{\sin\theta} + r + R$ ($\sin\theta \neq 0$ because $0° < \theta < 45°$). We also know $\sin\theta = \dfrac{QD}{OQ}$ and $QD = R$, so

$$\frac{R}{OQ} = \sin\theta = \frac{R}{\frac{r}{\sin\theta} + r + R}$$

Multiplying through by the denominator of the expression on the right gives

$$\begin{aligned} R &= \sin\theta\left(\frac{r}{\sin\theta} + r + R\right) \\ &= r + r\sin\theta + R\sin\theta. \end{aligned}$$

Bringing all terms with an R to one side and factoring, we get

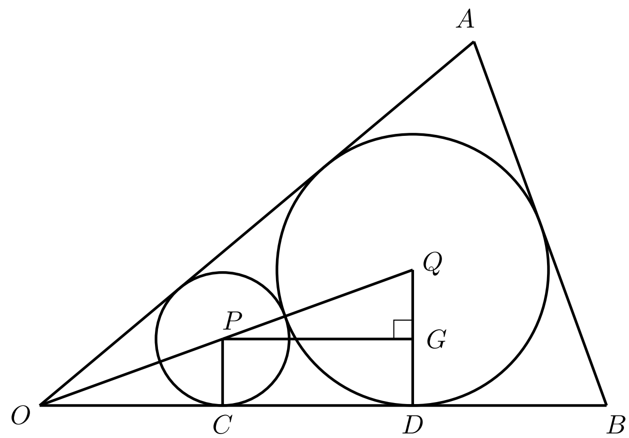
$$R(1 - \sin\theta) = r(1 + \sin\theta)$$

and so now we can solve for $\frac{R}{r}$ to get

$$\frac{R}{r} = \frac{1+\sin\theta}{1-\sin\theta}.$$

This expression is defined because $0 < \theta < 45°$, so $\sin\theta \neq 1$.

Solution 2: Let P and Q be the centres of the smaller and larger circles respectively, and let C and D be the points of tangency of the smaller and larger circles to OB. Let G be the point on QD so that PG is perpendicular to QD.



As mentioned in the first solution, $\angle PCD$ and $\angle QDC$ are both right angles and PQ passes through the point at which the two circles are tangent. As well, O, P, and Q lie on the angle bisector of $\angle AOB$.

This means PG is parallel to OD so $\angle QPG = \angle QOD$. We also have $\angle QGP = \angle QDO = 90°$, so $\triangle PQG$ is similar to $\triangle OQD$. Therefore, since Q lies on the angle bisector of $\angle AOB$, we have $\frac{QG}{PQ} = \frac{QD}{OQ} = \sin\theta$.

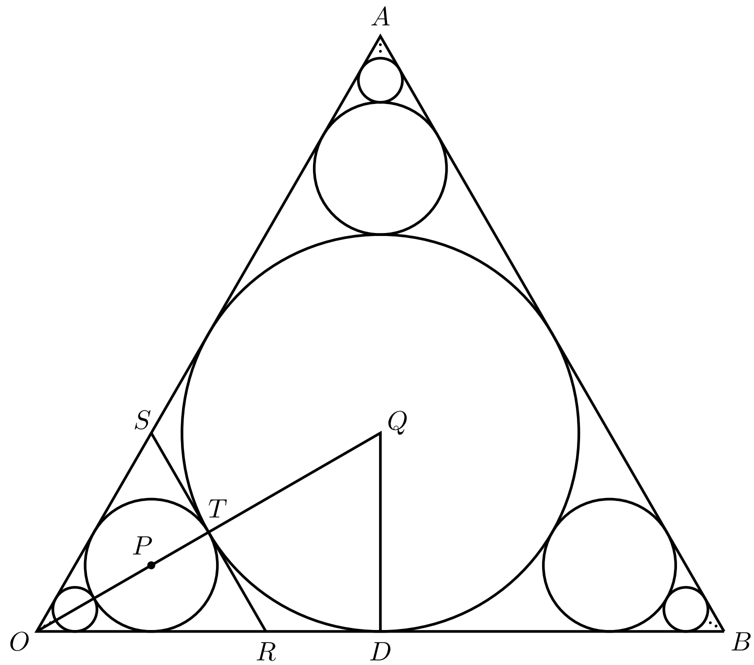
Let R be the radius of the larger circle and r be the radius of the smaller circle. Since quadrilateral $PGDC$ has three right angles, it is a rectangle, which means $GD = PC = r$. Thus, $QG = R - r$. We also have that $PQ = R + r$, so

$$\sin\theta = \frac{R-r}{R+r}.$$

This can be rearranged to get $R\sin\theta + r\sin\theta = R - r$ or $R(1-\sin\theta) = r(1+\sin\theta)$, and therefore

$$\frac{R}{r} = \frac{1+\sin\theta}{1-\sin\theta}.$$

2. We will label the triangle $\triangle OAB$. Let P be the centre of the largest circle in the bottom-left corner and Q be the centre of the largest circle. Let the circles with centres P and Q be tangent at T, and suppose the common tangent intersects OA at S and OB at R. Finally, let D be the point at which the circle centred at Q is tangent to OB.



By the reasoning in Question 1, points O, P, and Q all lie on the angle bisector of $\angle AOB$, so $\angle SOT = \angle ROT$. We also have, by circle properties, that $\angle STO = \angle RTO = 90°$. Therefore, $\triangle STO$ is congruent to $\triangle RTO$ by angle-side-angle congruence (these two triangles share side OT). It follows that $\angle OST = \angle ORT$ and since $\angle SOR = 60°$, we get that $\triangle SOR$ is equilateral. [Note: If we only assume that $\triangle AOB$ is isosceles, this argument still shows that $\triangle SOR$ is similar to $\triangle AOB$.]

Suppose the side lengths of $\triangle AOB$ are equal to x.

Since OQ is the angle bisector of $\angle AOB$, we have that $\angle QOD = \dfrac{60°}{2} = 30°$. Since OB is tangent to the largest circle at point D, we have that $\angle ODQ = 90°$. Therefore, $\triangle ODQ$ is a 30°-60°-90° triangle which implies $\dfrac{QD}{OD} = \dfrac{1}{\sqrt{3}}$. Since $\triangle AOB$ is equilateral, D is the midpoint of OB. [The proof of this is left as an exercise. One way to show it is to connect Q to B and show that $\triangle QOD$ is congruent to $\triangle QBD$.] This means $OD = \dfrac{x}{2}$ so $QD = \dfrac{x}{2\sqrt{3}}$. We have found the radius of the largest circle in terms of the side length of the triangle.

By Question 1 with $\theta = 30°$, the ratio of the radius of the circle centred at Q to the radius of the circle centred at P is

$$\frac{1+\sin 30°}{1-\sin 30°} = \frac{1+\frac{1}{2}}{1-\frac{1}{2}} = 3.$$

This means the radius of the circle centred at P is $\dfrac{1}{3} \times QD = \dfrac{x}{6\sqrt{3}}$. By symmetry, the other two circles tangent to the largest circle have this same radius.

We showed earlier that $\triangle SOR$ is equilateral. This means we can apply the argument above again to get that the radii of the three next largest circles are each $\dfrac{1}{3} \times \dfrac{x}{6\sqrt{3}}$. We could then draw the common tangent to the circle centred at P and the next largest circle to repeat the argument. The radius will be multiplied by $\frac{1}{3}$ each time.

Therefore, the total area of the circles is represented by the following infinite series:

$$\pi\left(\frac{x}{2\sqrt{3}}\right)^2 + 3\pi\left(\frac{x}{6\sqrt{3}}\right)^2 + 3\pi\left(\frac{x}{18\sqrt{3}}\right)^2 + \cdots.$$

The first term in the sum is equal to the area of the largest circle. The second term is equal to the total area of the three next largest circles (those tangent to the largest circle). The third term is equal to the total area of the three next largest circles, and so on.

After some simplification, the sum above is equivalent to

$$\frac{\pi x^2}{12} + \frac{3\pi x^2}{12}\left(\frac{1}{9} + \frac{1}{9^2} + \frac{1}{9^3} + \cdots\right).$$

If a and r are real numbers with $-1 < r < 1$, then we can find the sum of the geometric series $a + ar + ar^2 + \cdots$ using the formula $a + ar + ar^2 + \cdots = \dfrac{a}{1-r}$. Our expressions for the total area of the circles involves a geometric series with $a = r = \dfrac{1}{9}$, so

$$\frac{1}{9} + \frac{1}{9^2} + \frac{1}{9^3} + \cdots = \frac{\frac{1}{9}}{1-\frac{1}{9}} = \frac{1}{8}.$$

Therefore, the total area of the circles is

$$\begin{aligned}\frac{\pi x^2}{12} + \frac{3\pi x^2}{12} \times \frac{1}{8} &= \frac{8\pi x^2 + 3\pi x^2}{96} \\ &= \frac{11\pi x^2}{96}.\end{aligned}$$

There are several ways to determine the area of $\triangle AOB$ in terms of its side length, x. One way is to use that the area of a triangle with side lengths a and b meeting at angle α is $\dfrac{1}{2}ab\sin\alpha$. Thus, $\triangle AOB$ has area $\dfrac{1}{2}x^2\sin 60^\circ = \dfrac{\sqrt{3}x^2}{4}$ since each of its angles measures 60° and its sides all have length x. The fraction of the triangle that is covered by circles is

$$\frac{\frac{11\pi x^2}{96}}{\frac{\sqrt{3}x^2}{4}} = \frac{11\pi}{24\sqrt{3}}.$$

3. This calculation will be rather similar to the one in Question 2. Suppose the radius of the larger circle is R and set $\alpha = \dfrac{1-\sin\theta}{1+\sin\theta}$. From Question 1, we have that $\dfrac{r}{R} = \alpha$, or $r = \alpha R$. Following the reasoning in the solution to Question 2, we can show that the total area of the circles is given by

$$\pi R^2 + \pi(\alpha R)^2 + \pi(\alpha^2 R)^2 + \pi(\alpha^3 R)^2 + \cdots.$$

Factoring out πR^2, this is equal to

$$\pi R^2(1 + \alpha^2 + \alpha^4 + \alpha^6 + \cdots).$$

Since $0^\circ < \theta < 45^\circ$, we have that $0 < \sin\theta < 1$ (in fact, $\sin\theta < \frac{\sqrt{2}}{2}$, but having $\sin\theta < 1$ is good enough for what follows). This means $0 < 1 - \sin\theta < 1$. Furthermore, since $\sin\theta$ is positive, we have $1 - \sin\theta < 1 + \sin\theta$. It follows that

$$0 < \frac{1-\sin\theta}{1+\sin\theta} < 1$$

or $0 < \alpha < 1$ and so $0 < \alpha^2 < 1$. Therefore, using the formula for the sum of a geometric series (see Question 2), the total area of the circles is

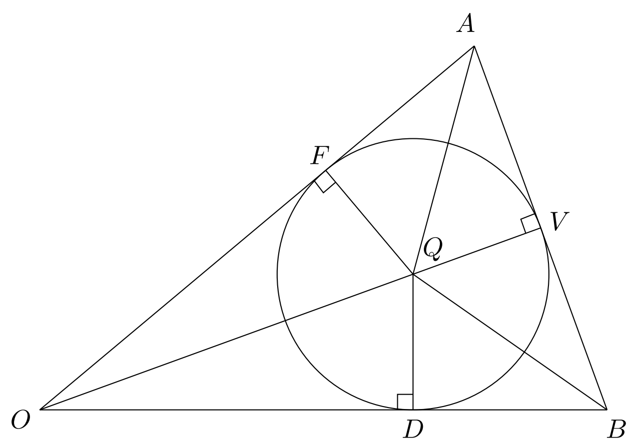
$$\pi R^2(1 + \alpha^2 + \alpha^4 + \alpha^6 + \cdots) = \frac{\pi R^2}{1-\alpha^2}.$$

Substituting the expression for α, we have that the total area of the circles is

$$\begin{aligned}\frac{\pi R^2}{1-\alpha^2} &= \frac{\pi R^2}{1 - \left(\frac{1-\sin\theta}{1+\sin\theta}\right)^2} \\ &= \frac{\pi R^2(1+\sin\theta)^2}{(1+\sin\theta)^2 - (1-\sin\theta)^2} \\ &= \frac{\pi R^2(1+\sin\theta)^2}{4\sin\theta}.\end{aligned}$$

We will return to the expression above later, but first we will find the area of $\triangle AOB$ in terms of R and θ in order to compute the ratio.

Let D, F, and V be the points of tangency of the largest circle to the three sides of $\triangle OAB$ as shown below. Connect the centre of the circle, Q, to O, A, B, D, F, and V. The rest of this page is devoted to proving that OQV is a line. You may wish to skip this part of the argument and come back to it later.



Similar to an observation in Question 1, we have that $OF = OD$ because they are equal tangents. Also, $QF = QD = R$ and $\triangle OQF$ and $\triangle OQD$ have common side OQ. By side-side-side congruence, $\triangle OQF$ is congruent to $\triangle OQD$. This means $\angle OQF = \angle OQD$.

By similar arguments, $\angle BQV = \angle BQD$ and $\angle AQV = \angle AQF$.

It is given that $OA = OB$, and since $OF = OD$, we have

$$FA = OA - OF = OB - OD = DB.$$

Again, $QF = QD = R$ and $\angle AFQ = \angle BDQ = 90^\circ$ because they are each made by a tangent and a radius, so we have that $\triangle AFQ$ is congruent to $\triangle BDQ$ by side-angle-side congruence. This means $\angle BQD = \angle AQF$.

Using that $\angle OQF = \angle OQD$ and that $\angle BQV = \angle BQD = \angle AQF = \angle AQV$, we get

$$\begin{aligned} 360^\circ &= \angle OQD + \angle BQD + \angle BQV + \angle AQV + \angle AQF + \angle OQF \\ &= \angle OQD + \angle BQD + \angle BQV + \angle BQV + \angle BQD + \angle OQD \\ &= 2(\angle OQD + \angle BQD + \angle BQV) \\ &= 2\angle OQV \end{aligned}$$

This means $\angle OQV = 180^\circ$, so OQV is a line segment.

By right-angle trigonometry and since the point Q lies on the angle bisector of $\angle AOB$, $\sin\theta = \dfrac{DQ}{OQ} = \dfrac{R}{OQ}$, so $OQ = \dfrac{R}{\sin\theta}$. Since $QV = R$ as well, we have that

$$OV = R + \frac{R}{\sin\theta}.$$

We also have that $\tan\theta = \dfrac{BV}{OV}$, which means

$$BV = OV\tan\theta = \left(R + \frac{R}{\sin\theta}\right)\tan\theta.$$

Since V is on the angle bisector of $\angle AOB$, we have $\angle AOV = \angle BOV$, so $\triangle AOV$ is congruent to $\triangle BOV$ by side-angle-side congruence. So, $AV = BV$ implying $AB = 2BV$. Therefore, the area of $\triangle OAB$ is

$$\begin{aligned} \frac{1}{2} \times AB \times OV &= \frac{1}{2} \times 2\left(R + \frac{R}{\sin\theta}\right)\tan\theta\left(R + \frac{R}{\sin\theta}\right) \\ &= R^2\tan\theta\left(1 + \frac{1}{\sin\theta}\right)^2. \end{aligned}$$

Recall that the total area of the circles is

$$\frac{\pi R^2(1+\sin\theta)^2}{4\sin\theta},$$

so the fraction of the triangle covered by circles is

$$\begin{aligned} \frac{\frac{\pi R^2(1+\sin\theta)^2}{4\sin\theta}}{R^2\tan\theta\left(1+\frac{1}{\sin\theta}\right)^2} &= \frac{\pi(1+\sin\theta)^2}{4\sin\theta\tan\theta\left(1+\frac{1}{\sin\theta}\right)^2} \\ &= \frac{\pi(1+\sin\theta)^2}{4\frac{\sin^2\theta}{\cos\theta}\left(1+\frac{1}{\sin\theta}\right)^2} \\ &= \frac{\pi\cos\theta(1+\sin\theta)^2}{4\left[\sin\theta\left(1+\frac{1}{\sin\theta}\right)\right]^2} \\ &= \frac{\pi\cos\theta(1+\sin\theta)^2}{4(1+\sin\theta)^2} \\ &= \frac{\pi}{4}\cos\theta. \end{aligned}$$

As mentioned in the statement of the problem, this result can be used to produce the answer from Question 2. We show how to do this now, noting that this isn't necessarily a better way to solve Question 2.

Suppose the side length of the equilateral triangle is x. We computed in Question 2 that the area of the triangle is $\dfrac{\sqrt{3}x^2}{4}$. As well, the area of the largest circle is $\dfrac{\pi x^2}{12}$.

In Question 2, there are three infinite "lines" of circles, each starting with the largest circle and extending toward a vertex of the triangle. By Question 3, each of these three lines of circles covers the fraction $\dfrac{\pi}{4}\cos\theta$ of the area of the triangle, where $\theta = \dfrac{60^\circ}{2} = 30^\circ$. Therefore, the area of each of the three infinite lines of circles is

$$\begin{aligned}\frac{\pi}{4}\cos 30^\circ \times \frac{\sqrt{3}x^2}{4} &= \frac{\pi}{4} \times \frac{\sqrt{3}}{2} \times \frac{\sqrt{3}x^2}{4} \\ &= \frac{3\pi x^2}{32}.\end{aligned}$$

If we take three times this quantity, we will have computed the total area of all circles in the picture from Question 2 but will have counted the area of the largest circle three times rather than once. Therefore, the total area of the circles is

$$\begin{aligned}3 \times \frac{3\pi x^2}{32} - 2 \times \frac{\pi x^2}{12} &= \pi x^2\left(\frac{9}{32} - \frac{1}{6}\right) \\ &= \pi x^2\left(\frac{27}{96} - \frac{16}{96}\right) \\ &= \frac{11\pi x^2}{96}.\end{aligned}$$

Therefore, the fraction of the triangle covered by circles is

$$\frac{\frac{11\pi x^2}{96}}{\frac{\sqrt{3}x^2}{4}} = \frac{11\pi}{24\sqrt{3}}$$

which is indeed the answer from Question 2.

Problem of the Month

Problem 3: Multiplication in two dimensions

December 2025

This month's problem is inspired by Question B2(c) on the 2025 Canadian Senior Mathematics Contest. Here is the original question:

> The points X, Y, and Z have coordinates $X(0,0)$, $Y(7,24)$, and $Z(15,0)$. The point W is on the line segment YZ such that $\angle WXZ = 3\angle WXY$. Determine the coordinates of W.

Give it a try as a warm up before reading on!

One path to solving this problem is to introduce a point V on the line segment YZ so that $\angle VXZ = \angle VXY$. If you do this, you find the coordinates of V are $(12,9)$. These are very nice numbers! In this month's POTM, we will investigate how the points X, Y, and Z were chosen so that the coordinates of V (and eventually W) are nice rational numbers. This will involve a way to multiply points on the Cartesian plane.

1. Given points (a,b) and (c,d) on the Cartesian plane, define their *product* as

$$(a,b) * (c,d) = (ac - bd, ad + bc).$$

   So, for example, $(3,5) * (2,-1) = (3 \cdot 2 - 5 \cdot (-1), 3 \cdot (-1) + 5 \cdot 2) = (11,7)$.

   (a) Find a point (a,b) satisfying $(1,1) * (a,b) = (0,-2)$.

   (b) Find a point (a,b) with the property that $(a,b) * (c,d) = (c,d)$ for every point (c,d) in the Cartesian plane.

2. For a point (a,b) in the Cartesian plane, denote by $(a,b)^k$ the point obtained by taking the product of (a,b) with itself k times. Compute $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^{2025}$.

3. Denote by O the origin $(0,0)$, and by E the point with coordinates $(1,0)$. Let A be a point in the Cartesian plane. Define $|A|$ to be the distance from A to O. Define $\theta(A)$ to be the measure of the angle $\angle EOA$, measured counterclockwise around O from the line segment OE. For example, $|(-\sqrt{2},-\sqrt{2})| = \sqrt{(-2)^2 + (-2)^2} = 2$ and $\theta(-\sqrt{2},-\sqrt{2}) = 225°$.

   (a) Compute $|(0,2) * (1,1)|$ and $\theta((0,2) * (1,1))$.

   (b) Let D_1 and D_2 be points with $|D_1| = r_1$, $|D_2| = r_2$, $\theta(D_1) = \phi_1$ and $\theta(D_2) = \phi_2$. Compute $|D_1 * D_2|$ and $\theta(D_1 * D_2)$ in terms of r_1, r_2, ϕ_1, and ϕ_2.

4. The point $(2,3)$ satisfies the equation $x^4 = (-119,-120)$ since $(2,3)^4 = (-119,-120)$. Find three other points satisfying $x^4 = (-119,-120)$.

5. Let Y have coordinates $(7,24)$. Find a point F in the Cartesian plane with integer coordinates so that $OF^2 = OY$ and $2\angle EOF = \angle EOY$.

Problem of the Month

Problem 3: Multiplication in two dimensions

December 2025

Hint

1. (a) Expand out the left-hand side, and equate it to the right-hand side of the given equation.

   (b) If it's true for all (c, d) it must be true when $(c, d) = (1, 1)$ (or any other specific point).

2. Compute the first six powers and plot them on the Cartesian plane. Question 1(b) may come in handy here.

3. For both (a) and (b), it may help to plot $(0, 2), (1, 1)$, and $(0, 2) * (1, 1)$ on the Cartesian plane. For (b), try to write the coordinates of D_1 in terms of r_1 and ϕ_1. To do this, begin by assuming D_1 is in the first quadrant of the Cartesian plane and draw out a diagram relating r_1, θ_1, and the coordinates of D_1.

4. Suppose C is a solution to $x^4 = (-119, -120)$. Using 3(b), see if you can figure anything out about $|C|$ and $\theta(C)$.

5. Interpret the conditions given in the question in terms of $|F|$, $|Y|$, $\theta(F)$, and $\theta(Y)$. Then apply 3(b).

Problem of the Month

Solution to Problem 3: Multiplication in two dimensions

December 2025

1. (a) We have $(1, 1) * (a, b) = (a - b, a + b) = (0, -2)$. This gives us the simultaneous linear equations $a - b = 0$ and $a + b = -2$. The first equation gives $a = b$. Substituting into the second equation we get $2a = -2$ and so $a = b = -1$. Therefore $(a, b) = (-1, -1)$.

   (b) Since $(a, b) * (c, d) = (c, d)$ for all points (c, d), we must have $(a, b) * (1, 0) = (1, 0)$. The definition of the product gives $(a, b) * (1, 0) = (a, b)$. Therefore $(a, b) = (1, 0)$ is a good candidate for an answer! Let's check that it works. We have

$$(1, 0) * (c, d) = (1c - 0d, 1d + 0c) = (c, d),$$

   so the answer is $(a, b) = (1, 0)$.

2. Before we get stuck into the solution, there is a subtle point about the product $*$ that we need to sort out. The expression $(a, b)^4$ is defined to mean the product of (a, b) with itself four times. But what does this mean exactly? Does it mean $[(a, b) * (a, b)] * [(a, b) * (a, b)]$ or $(a, b) * [(a, b) * [(a, b) * (a, b)]]$, or anything else? Does it even matter?

   We will see in a moment, just like with multiplication of real numbers, that how we group such a product doesn't affect the outcome. Let's prove that now. Let $(a, b), (c, d), (e, f)$ be three points in the Cartesian plane. Then

$$\begin{aligned} [(a, b) * (c, d)] * (e, f) &= (ac - bd, ad + bc) * (e, f) \\ &= ((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e) \\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce). \end{aligned}$$

   Also,

$$\begin{aligned} (a, b) * [(c, d) * (e, f)] &= (a, b) * (ce - df, cf + de) \\ &= (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)) \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf) \\ &= [(a, b) * (c, d)] * (e, f). \end{aligned}$$

   We have just proved that for a product of three points, the grouping of the three points does not matter. That is, it doesn't matter if you first take the product of the first two, and then the third, or if you first take the product of the last two, and then the first. In fancy math terminology, we have proved that the product $*$ is *associative*.

   Since the product $*$ is associative, we can take powers without worrying about how we're grouping the product. We can now safely move on to the question.

Let's compute the first few powers of $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.

$$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^2 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$$
$$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^3 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) * \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = (-1, 0)$$
$$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^4 = (-1, 0) * \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$$
$$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^5 = \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) * \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$$
$$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^6 = \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) * \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = (1, 0).$$

We know from 1(b) above that $(1,0) * (c,d) = (c,d)$ for any point (c,d). Therefore, for any integer $k > 6$, we have

$$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^k = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^6 * \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^{k-6} = (1,0) * \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^{k-6} = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^{k-6}.$$

So, to compute a power of 2025, we can keep subtracting 6 from 2025 until we get to a power that we have already computed. Since $2025 = 337 \cdot 6 + 3$ we have

$$\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^{2025} = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^{2019} = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^{2013} = \cdots = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)^3 = (-1, 0).$$

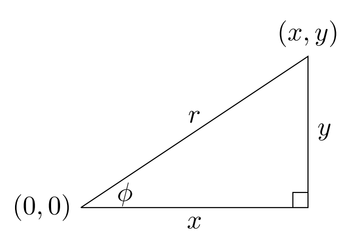
3. (a) We first compute $(0,2) * (1,1) = (-2,2)$. Then

$$|(0,2) * (1,1)| = |(-2,2)| = \sqrt{(-2)^2 + 2^2} = \sqrt{8} = 2\sqrt{2}.$$

Also, $\theta((0,2) * (1,1)) = \theta(-2,2)$. The point $(-2,2)$ lies in the second quadrant of the Cartesian plane on the line $y = -x$, which is at $45°$ to the y-axis. Therefore $\theta(-2,2) = 90° + 45° = 135°$.

(b) A very helpful thing for this question is to first write the coordinates of each point in terms of r_i and ϕ_i. Let's start with points in the first quadrant.

Suppose x and y are positive real numbers, $|(x,y)| = r$, and $\theta(x,y) = \phi$. Then we have the following diagram.



Therefore, $x = r\cos(\phi)$ and $y = r\sin(\phi)$. Miraculously, these equations hold in every quadrant, and on the x- and y-axes. It is left up to you to check the details of this.

So, the coordinates of D_1 and D_2 are $(r_1\cos(\phi_1), r_1\sin(\phi_1))$ and $(r_2\cos(\phi_2), r_2\sin(\phi_2))$ respectively. Let's see what happens when we take the product of D_1 and D_2. We have

$$\begin{aligned}
&(r_1\cos(\phi_1), r_1\sin(\phi_1)) * (r_2\cos(\phi_2), r_2\sin(\phi_2)) \\
&= (r_1r_2\cos(\phi_1)\cos(\phi_2) - r_1r_2\sin(\phi_1)\sin(\phi_2), r_1r_2\cos(\phi_1)\sin(\phi_2) + r_1r_2\sin(\phi_1)\cos(\phi_2)) \\
&= (r_1r_2\cos(\phi_1+\phi_2), r_1r_2\sin(\phi_1+\phi_2))
\end{aligned}$$

where the last equality uses the angle sum formulas for sine and cosine. Therefore, $|D_1 * D_2| = r_1r_2$ and $\theta(D_1 * D_2) = \phi_1 + \phi_2$. The moral of the story is that when you take the product of two points, their distances multiply and their angles (when measured counterclockwise from the positive x-axis) add.

4. The three other points are $(-3,2), (-2,-3)$, and $(3,-2)$ (you can check that these are indeed solutions by computing $(-3,2)^4$, for example). Here is one way we could have found these points.

   Suppose C is a solution to $x^4 = (-119,-120)$. Then we know $|C|^4 = |(-119,-120)|$ by Question 3(b). However, $|(2,3)|^4 = |(-119,-120)|$ and so $|C|^4 = |(2,3)|^4$. Since both $|C|$ and $|(2,3)|$ are non-negative real numbers, it must be the case that $|C| = |(2,3)|$.

   So, we know how far away from the origin any solution to $x^4 = (-119,-120)$ must be, we just need to figure out which directions to go from the origin to find solutions.

   Using the result from 3(b) again, we know that $4\cdot\theta(C) = \theta(-119,-120) = 4\cdot\theta(2,3)$. It's tempting to think that we can therefore conclude that $\theta(C) = \theta(2,3)$, but this is not the case!

   However, since $4\cdot\theta(C)$ gives the same direction from the origin as $4\cdot\theta(2,3)$, it must be that $4\cdot\theta(C)$ and $4\cdot\theta(2,3)$ differ by a multiple of $360°$. This occurs precisely when $\theta(C)$ and $\theta(2,3)$ differ by a multiple of $90°$.

   Putting all of this together, to find other solutions to $x^4 = (-119,-120)$, we can take the given solution and rotate it counterclockwise about the origin by $90°$, $180°$, and $270°$.

   The points $(-3,2)$, $(-2,-3)$, and $(3,-2)$ are the result of rotating the given solution $(2,3)$ by $90°$, $180°$, and $270°$ counterclockwise about the origin respectively.

   In fact, the argument above proves that these are *all* the possible solutions the given equation. Can you see why?

5. Although this appears to be a problem in Euclidean geometry, we can approach it using properties of the product of points on the Cartesian plane. Note that $OF = |F|$, $OY = |Y|$, $\angle EOF = \theta(F)$ and $\angle EOY = \theta(Y)$.

   Therefore, the conditions given in the problem are asking us to find a point F satisfying $|F|^2 = |Y|$ and $2\theta(F) = \theta(Y)$. By 3(b) above, a point F satisfying $F * F = Y$ will do the trick!

   We compute $|Y| = \sqrt{7^2 + 24^2} = 25$. Therefore, we are looking for a point F satisfying $|F| = 5$. Suppose F has coordinates (x,y). The question specifies that F has integer coordinates, so we are looking for integers x and y such that $\sqrt{x^2+y^2}=5$. There are not very many pairs of integers to check here! We must have that x and y are, in some order ± 3 and ± 4, or 0 and ± 5.

We have $(\pm 5, 0)^2 = (25, 0)$ and $(0, \pm 5)^2 = (-25, 0)$. Neither of these are the point $(7, 24)$. Trying $(x, y) = (3, 4)$ we get $(3, 4)^2 = (-7, 24)$. Close, but not quite. Finally, we have $(4, 3)^2 = (7, 24)$, which is what we are after! Therefore the point F with coordinates $(4, 3)$ is a solution to the problem.

Now that you've gone through all of this, can you see how Question B2(c) could have been created?

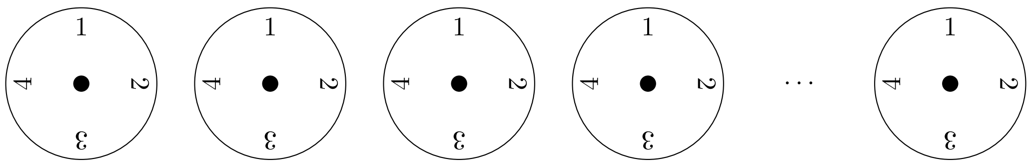
For those of you that are familiar with complex numbers, the product in the question is secretly multiplication of complex numbers. Can you see how?

Problem of the Month

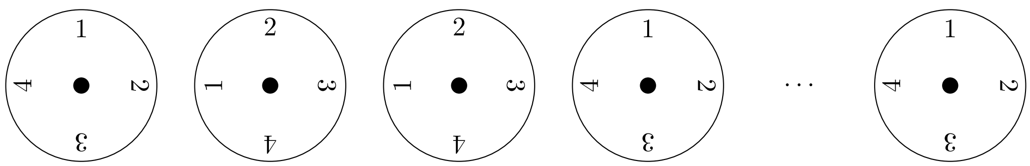
Problem 4: Rotating dials

January 2026

1. Several dials are each labelled with the integers from 1 through 4 in clockwise order. The dials are arranged in a row and initially configured so that each dial shows 1 at the top:



A *move* consists of rotating two adjacent dials in the same direction by the same number of positions. For example, one possible move is to rotate the second and third dials by one position in the counterclockwise direction resulting in the configuration shown:



There are $k \geq 2$ dials and they are initially configured so that each shows 1 at the top. In terms of k, determine how many possible configurations of the dials are attainable by performing a sequence of moves.

2. Suppose now that there is an integer $n \geq 2$ so that each of the $k \geq 2$ dials is labelled in clockwise order by the integers 1 through n beginning with 1 at the top. Find the number of configurations of the dials that are attainable by a sequence of moves. Your answer should be in terms of n and k. Again, a move consists of rotating two adjacent dials in the same direction by the same number of positions.

3. Answer Question 2 with the following additional type of move allowed: rotate the leftmost and rightmost dials in the same direction by the same number of positions.

Problem of the Month

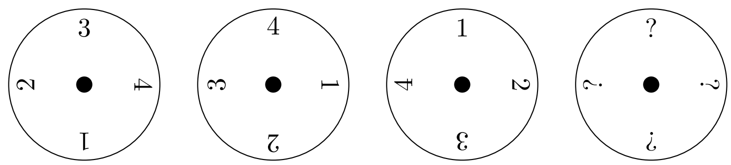
Problem 4: Rotating dials

January 2026

Hint

Here are two distinct but related hints for this problem:

- Does the order in which moves are applied affect the outcome of a sequence of moves?
- Suppose $k = 4$ and the dials are configured as follows:



  Is it possible to determine the position of the 4^{th} dial?

Problem of the Month

Solution to Problem 4: Rotating dials

January 2026

1. We first observe that if a sequence of moves is performed, the order in which the moves are performed does not affect the overall outcome. To prove this, it is enough to show that if two different moves are performed in either order, the same result is achieved.

   Suppose Move A and Move B both involve the i^{th} dial. In particular, let us suppose Move A rotates the i^{th} dial by a positions and Move B rotates the i^{th} dial by b positions. Here, a and b are allowed to be integers and a negative integer represents a counterclockwise rotation. The net effect of Move A followed by Move B on the i^{th} dial is a rotation by $a+b$ positions. The net effect of Move B followed by Move A is a rotation by $b+a=a+b$ positions. Therefore, the net effect on the i^{th} dial is the same regardless of the order in which the moves are performed.

   If the i^{th} dial is affected by Move A and not by Move B, then the net effect of Move A and Move B on the i^{th} dial is the same as the effect of Move A, regardless of the order. Similarly, if the i^{th} dial is affected by Move B and not by Move A, then the net effect is the same regardless of the order in which the moves are performed.

   Of course, if neither Move A nor Move B has any effect on the i^{th} dial, then the effect of Move A and Move B on the i^{th} dial is the same regardless of the order in which the moves are performed.

   It follows that the final state of the dials only depends on which moves were performed and not on the order in which they were performed. Also, there is no reason to rotate the same pair of dials twice since the same effect could be achieved with a single rotation. Furthermore, there is no reason to rotate the same pair of dials by more than three positions in either direction since this would result in the dial going all the way around at least once. The same effect could be achieved using a rotation by fewer positions. Finally, the effect of a rotation in the counterclockwise direction can be achieved by a rotation in the clockwise direction (possibly by a different number of positions). Therefore, there is no reason to rotate any pair of dials in the counterclockwise direction.

   There are $k-1$ possible pairs of dials that can be rotated. Each pair may be not rotated at all, rotated clockwise by one position, rotated clockwise by two positions or rotated clockwise by three positions. As mentioned in the previous paragraph, any other move on a pair of dials has the same effect on the dials as one of these four moves. Therefore, there are a total of four possible moves that can be performed on each of the $k-1$ pairs of dials. This means any final configuration that can be achieved by a sequence of moves can be achieved by one of these 4^{k-1} sets of moves.

   It is possible that two sets of moves lead to the same final configuration, so we have merely established that there are at most 4^{k-1} attainable configurations.

   Suppose $a_1, a_2, \ldots, a_{k-1}$ is a sequence with a_r taking one of the values $1, 2, 3$, or 4 for each $1 \leq r \leq k-1$. There are 4^{k-1} such sequences. By rotating the first two dials, we can make the number on top of the first dial equal to a_1. This will also rotate the second dial, but we can now rotate the second and third dials to get the second dial to have a_2 at the top. Furthermore, this will not change the number at the top of the first dial. Continuing in this way, we can rotate the third and fourth dials to get the third dial to have a_3 at the top without changing the first two dials. This can be continued to get a_r on the top of dial r for $1 \leq r \leq k-1$. Regardless of the position of the k^{th} dial, this gives a way to produce at least 4^{k-1} different configurations since any two of these configurations differ on at least one of the first $k-1$ dials.

Therefore, there are at least 4^{k-1} configurations. Since there are also at most 4^{k-1} configurations, this means there are exactly 4^{k-1} configurations.

2. As in Question 1, the order in which moves are applied does not matter. It only matters which moves are applied.

   There are $k-1$ possible pairs of dials to be rotated and n possible positions by which to rotate each pair. As in Question 1, the effect of any number of rotations of the same pair of dials can be achieved by a single clockwise rotation. Following a similar argument to the one in Question 1 (with 4 replaced by n), this means there are no more than n^{k-1} possible configurations.

   Also similar to Question 1, the first $k-1$ dials can be configured in any of the n^{k-1} possible ways (though without control over the k^{th} dial). This shows that there are at least n^{k-1} configurations.

   Since there are also at most n^{k-1} attainable configurations, there must be exactly n^{k-1} attainable configurations.

3. We first suppose k is even. Consider the following sequence of moves, each by one position:

Dials	Direction
1 and 2	clockwise
2 and 3	counterclockwise
3 and 4	clockwise
4 and 5	counterclockwise
$\vdots$	$\vdots$
$k-2$ and $k-1$	counterclockwise
$k-1$ and k	clockwise

   This alternating pattern ends up with the final move being clockwise because k is even. Each of dials 2 through $k-1$ has been rotated by one position clockwise and one position counterclockwise. Therefore, the net effect of this sequence of moves is to rotate dials 1 and k clockwise by one position and to leave all other dials in their original position. This sequence of moves could be repeated to attain any configuration achievable by the new type of move. Therefore, the new type of move can be mimicked by the original moves, so including it does not introduce any new attainable configurations.

   Thus, when k is even, the number of configurations is n^{k-1}.

   We now suppose k and n are odd and perform an "alternating" sequence of moves like in the previous case. Again, each move is by one position:

Dials	Direction
1 and 2	clockwise
2 and 3	counterclockwise
3 and 4	clockwise
4 and 5	counterclockwise
$\vdots$	$\vdots$
$k-2$ and $k-1$	clockwise
$k-1$ and k	counterclockwise
k and 1	clockwise

Since k is odd, this alternating pattern leads to dials $k-1$ and k being rotated counterclockwise, and finally dials k and 1 being rotated clockwise. The net effect of this sequence of moves is that dial 1 is rotated clockwise by two positions and all other dials are unchanged.

Since n is odd, $n+1$ is even, which means $\frac{n+1}{2}$ is an integer. If the sequence of moves above is repeated $\frac{n+1}{2}$ times, the net effect will be to rotate the first dial by $2\left(\frac{n+1}{2}\right) = n+1$ positions clockwise, which is the same as rotating by one position clockwise.

By repeating everything that has been done so far, we can independently move the first dial to any position we like without changing the position of any other dials.

Now imagine performing a new sequence of moves similar to those in the table above by increasing each integer in the above table by 1, with the exception of k which we change to 1. This modified sequence of moves will rotate dial 2 by two positions clockwise and have no overall effect on any other dial. Using the same reasoning as in the previous paragraph, this modified sequence can be repeated $\frac{n+1}{2}$ times to have the effect of rotating dial 2 clockwise by one position. Repeating all of this as many times as desired, we can achieve the effect of rotating dial 2 by any number of positions without rotating any other dials.

This can be repeated for any other dial. In other words, with the new type of move, each dial can be moved to any position without changing any of the others.

Therefore, when k and n are both odd, each of the n^k configurations of the dials is attainable.

Finally, we consider the case when k is odd and n is even. As with the case when k and n are both odd, it is still possible to rotate any individual dial by exactly two positions clockwise without changing the position of any other dial. If you read that part of the argument closely, you will notice that it only relied on the fact that k was odd and was independent of n.

Similar to the argument used for Questions 1 and 2, by only using the original allowed moves, we can get the dials to a configuration where the first $k-1$ dials are in any positions we like. Furthermore, since we can rotate the k^{th} dial by multiples of two positions clockwise, there are $\frac{n}{2}$ positions of the k^{th} dial for each of the n^{k-1} configurations of the first $k-1$ dials. This means there are at least

$$\frac{n}{2}\left(n^{k-1}\right) = \frac{n^k}{2}$$

attainable configurations.

We will now argue that there are at most $\frac{n^k}{2}$ configurations.

Notice that in the initial configuration, the sum of the numbers showing at the top of each dial is $k \times 1 = k$ which we are assuming is odd. Each move changes two dials by the same amount, which means it adds or subtracts an even number from the total of the numbers on the top of the dials. Therefore, every attainable configuration must have the property that the total of the numbers showing on the top of the dials is odd.

Since n is even, exactly $\frac{n}{2}$ of the integers in the list $1, 2, 3, 4, \ldots, n$ are even, and exactly $\frac{n}{2}$ are odd. Suppose the dials are configured in some way and for each r with $1 \leq r \leq k-1$, the number showing at the top of the r^{th} dial is a_r. If $a_1 + a_2 + \cdots + a_{k-1}$ is even, then turning the k^{th} dial so that any of the $\frac{n}{2}$ numbers $1, 3, 5, \ldots, n-1$ is at the top will make the sum of the numbers of the top of all k dials odd. Turning the k^{th} dial to any of the other $\frac{n}{2}$ positions will make the total even. Similarly, if $a_1 + a_2 + \cdots + a_{k-1}$ is odd, then setting the k^{th} dial to have any of $2, 4, 6, \ldots, n$ at the top will make the total odd, and setting it to any of $1, 3, 5, 7, \ldots, n-1$ will make the total odd.

Either way, for any of the n^{k-1} configurations of the first $k-1$ dials, there are $\frac{n}{2}$ ways to arrange the k^{th} dial to make the sum of the numbers at the top of the dials odd, and $\frac{n}{2}$ ways to make the sum even. This means there are at least $\frac{n^k}{2}$ configurations with the sum of the top numbers being odd, and at least $\frac{n^k}{2}$ with the sum of the top numbers being even. Since $\frac{n^k}{2} + \frac{n^k}{2} = n^k$, this accounts for all configurations of the k dials. Therefore, there are exactly $\frac{n^k}{2}$ configurations of the dials for which the sum of the entries at the top of the dials is odd.

This implies there are at most $\frac{n^k}{2}$ attainable configurations, so there are exactly $\frac{n^k}{2}$ attainable configurations. The following table summarizes the results we have collected:

k	n	# of attainable configurations
even	even	n^{k-1}
even	odd	n^{k-1}
odd	even	$\dfrac{n^k}{2}$
odd	odd	n^k

Problem of the Month

Problem 5: Stabilising Sequences

February 2026

Suppose you have an infinite sequence $a_0, a_1, a_2, \ldots$ of real numbers. We can consider the differences between consecutive terms in the sequence to get a new sequence. We can then consider differences between terms in the new sequence, to get yet another sequence, and so on! To keep track of all of this, for all integers $n \geq 0$ and $k \geq 0$ define

$$a_n^{(0)} = a_n \quad \text{and} \quad a_n^{(k)} = a_{n+1}^{(k-1)} - a_n^{(k-1)}.$$

For example, if the original sequence is given by $a_n = n^2$, then

$$\begin{aligned}(a_0, a_1, a_2, a_3, \ldots) = \left(a_0^{(0)}, a_1^{(0)}, a_2^{(0)}, a_3^{(0)}, \ldots\right) &= (0, 1, 4, 9, \ldots) \\ \left(a_0^{(1)}, a_1^{(1)}, a_2^{(1)}, a_3^{(1)}, \ldots\right) &= (1, 3, 5, 7, \ldots) \\ \left(a_0^{(2)}, a_1^{(2)}, a_2^{(2)}, a_3^{(2)}, \ldots\right) &= (2, 2, 2, 2, \ldots).\end{aligned}$$

Note that the superscripts (for example the (2) in $a_1^{(2)}$) are *not* exponents, but just notation to keep track of everything.

We say a sequence $a_0, a_1, a_2, \ldots$ *stabilises at layer* k if k is the smallest integer for which $a_n^{(k)} = a_{n+1}^{(k)}$ for all $n \geq 0$. For example, the sequence $a_0, a_1, a_2, \ldots$ defined by $a_n = n^2$ stabilises at layer 2.

1. A sequence that stabilises at layer 1 begins with $a_0 = 5$ and $a_1 = 8$. Compute a_{2026}.
2. The sequence $a_0, a_1, a_2, \ldots$ defined by $a_n = 7n^4$ stabilises at layer k. Find k and compute $a_n^{(k)}$ for every integer $n \geq 0$.
3. A sequence $a_0, a_1, a_2, \ldots$ is defined by $a_n = C_t n^t + C_{t-1} n^{t-1} + C_{t-2} n^{t-2} + \cdots + C_1 n + C_0$ for some integer $t \geq 0$ and some constant real numbers $C_0, C_1, \ldots, C_t$ with $C_t \neq 0$. Show that the sequence stabilises at layer k for some k, and compute $a_n^{(k)}$ for every integer $n \geq 0$.
4. A sequence that stabilises at layer 3 begins with $a_0 = 7$, $a_1 = 5$, $a_2 = 13$, and $a_3 = 43$. Compute a_{2026}.

Problem of the Month

Problem 5: Stabilising Sequences

February 2026

Hint

1. First compute $a_0^{(1)}$ and $a_1^{(1)}$, and use this to compute a_2. Can you then compute a_3?
2. Start by computing a_0, a_1, a_2, a_3, a_4, and a_5. Use these to compute the first few terms of the next layer (i.e., the terms $a_0^{(1)}, a_1^{(2)}, \ldots$). Then compute the first few terms of the next layer, and then the next layer. Keep going until you think you've reached the layer at which the sequence stabilises.
3. Try some specific examples of sequences like this. You already did one in Question 2. Try $a_n = n^2 + 3n + 2$ and $a_n = n^3 - n$. Explicitly compute expressions for the next few layers and pay attention to the degree of the polynomial that emerges at each layer.
4. Use Question 3 to guess at a general form for a_n.

Problem of the Month

Solution to Problem 5: Stabilising Sequences

February 2026

1. For this sequence we have $a_0^{(1)} = a_1 - a_0 = 8 - 5 = 3$. Since the sequences stabilises at layer 1, we have $a_n^{(1)} = 3$ for all n. Therefore, for all integers $n \geq 0$, $a_{n+1} - a_n = 3$, or equivalently, $a_{n+1} = a_n + 3$. So, each term is three more than the term before it. Since $a_0 = 5$, we have

$$\begin{aligned} a_1 &= 5 + 3 \\ a_2 &= 5 + 2 \cdot 3 \\ a_3 &= 5 + 3 \cdot 3 \\ a_4 &= 5 + 4 \cdot 3 \end{aligned}$$

and so on. Therefore, $a_{2026} = 5 + 3 \cdot 2026 = 6083$.

2. Let's explicitly compute $a_n^{(k)}$ for the first few values of k. For all integers $n \geq 0$ we have

$$\begin{aligned} a_n^{(1)} &= a_{n+1} - a_n \\ &= 7(n+1)^4 - 7n^4 \\ &= 7n^4 + 28n^3 + 42n^2 + 28n + 7 - 7n^4 \\ &= 28n^3 + 42n^2 + 28n + 7. \end{aligned}$$

Then

$$\begin{aligned} a_n^{(2)} &= a_{n+1}^{(1)} - a_n^{(1)} \\ &= 28(n+1)^3 + 42(n+1)^2 + 28(n+1) + 7 - 28n^3 - 42n^2 - 28n - 7 \\ &= 84n^2 + 84n + 28 + 84n + 48 + 28 + 7 \\ &= 84n^2 + 168n + 111. \end{aligned}$$

Continuing in this manner,

$$\begin{aligned} a_n^{(3)} &= a_{n+1}^{(2)} - a_n^{(2)} \\ &= 84(n+1)^2 + 168(n+1) + 111 - 84n^2 - 168n - 111 \\ &= 168n + 84 + 168 \\ &= 168n + 252. \end{aligned}$$

Finally,

$$\begin{aligned} a_n^{(4)} &= a_{n+1}^{(3)} - a_n^{(3)} \\ &= 168(n+1) + 252 - 168n - 252 \\ &= 168. \end{aligned}$$

We have that $a_n^{(4)} = a_{n+1}^{(4)} = 168$ for all integers $n \geq 0$ and $k = 4$.

3. We will take inspiration for this solution from our solution to Question 2. In the solution above, notice that the expression for each sequence $a_n^{(\ell)}$ was always a polynomial, and the degree of the polynomial defining $a_n^{(\ell+1)}$ is one less than the degree of the polynomial defining $a_n^{(\ell)}$. Let's prove this in general.

   Suppose for some integer $\ell \geq 0$, $a_n^{(\ell)} = Cn^d + P(n)$, where C is some constant real number other than 0, $d \geq 0$ is an integer, and $P(n)$ is a polynomial in n of degree at most $d-1$.

   To understand this notation a little more, let's look at a specific example. If, for example, $a_n^{(\ell)} = 4n^3 + n^2 - n - 1$, we would have $C = 4$, $d = 3$, and $P(n) = n^2 - n - 1$. Notice that $P(n)$ is a polyomial of degree 2 (that is the highest power of n that occurs is 2), and $2 < d$.

   Great! So, we assume that $a_n^{(\ell)} = Cn^d + P(n)$. Then

$$a_n^{(\ell+1)} = a_{n+1}^{(\ell)} - a_n^{(\ell)} = C(n+1)^d + P(n+1) - Cn^d - P(n).$$

   To proceed, we will need two facts about the behaviour of polynomials. The proofs of these facts will be deferred to the end of this document, but see if you can prove them yourself first!

   Fact 1: For all integers $d \geq 1$, $(n+1)^d = n^d + dn^{d-1} + P(n)$ where $P(n)$ is a polynomial of degree at most $d-2$.

   Fact 2: If $P(n)$ is a polynomial of degree d, then $P(n+1) - P(n)$ is a polynomial of degree at most $d-1$.

   With these facts in hand let's continue. We have

$$\begin{aligned}
a_n^{(\ell+1)} &= C(n+1)^d + P(n+1) - Cn^d - P(n) \\
&= Cn^d + dCn^{d-1} + Q(n) + P(n+1) - Cn^d - P(n) \\
&= dCn^{d-1} + Q(n) + P(n+1) - P(n)
\end{aligned}$$

   where $Q(n)$ is some polynomial of degree at most $d-2$. Since $P(n)$ has degree at most $d-1$, Fact 2 implies that $P(n+1) - P(n)$ has degree at most $d-2$. Therefore, we can conclude that $R(n) = Q(n) + P(n+1) - P(n)$ is a polynomial of degree at most $d-2$. Putting all of this together, $a_n^{(\ell+1)} = dCn^{d-1} + R(n)$ where $R(n)$ is a polynomial of degree at most $d-2$. We have just proved the following result:

   Result 1: If $a_n^{(\ell)} = Cn^d + P(n)$ where $P(n)$ is a polynomial of degree at most $d-1$, then $a_n^{(\ell+1)} = dCn^{d-1} + R(n)$ where $R(n)$ is a polynomial of degree at most $d-2$.

   With Result 1 in hand, let's attack the original problem. We are given that $a_n^{(0)} = C_t n^t + P(n)$ for some polynomial $P(n)$ of degree at most $t-1$ (it could be the case that $C_{t-1} = 0$, so the degree may be less than $t-1$). Applying Result 1 repeatedly we get

$$\begin{aligned}
a_n^{(1)} &= tC_t n^{t-1} + P_1(n) \\
a_n^{(2)} &= (t-1)tC_t n^{t-2} + P_2(n) \\
a_n^{(3)} &= (t-2)(t-1)tC_t n^{t-3} + P_3(n) \\
&\vdots \\
a_n^{(t-1)} &= (2)(3)\cdots(t-2)(t-1)tC_t n + P_{t-1}(n)
\end{aligned}$$

where $P_r(n)$ is a polynomial of degree at most $t-r-1$. Since $P_{t-1}(n)$ is a polynomial of degree at most $t-(t-1)-1=0$, it must just be some real number K. Rewriting our expression for $a_n^{(t-1)}$ a little we have

$$a_n^{(t-1)} = (t!)C_t n + K.$$

We can now explicitly compute $a_n^{(t)} = (t!)C_t(n+1) + K - (t!)C_t n - K = (t!)C_t$ for all n, which is constant! We can conclude that the sequence stabilises at layer t.

4. We will approach this problem in two steps. Step one will be to show that the first four terms determine all the terms in the sequence. Step two will be to use Question 3 to find a general expression for such a sequence that stabilises at layer 3, and has the first four terms given in the statement of the question.

   For step one, assume $n \geq 4$. Then

$$\begin{aligned} a_{n-4}^{(3)} &= a_{n-3}^{(2)} - a_{n-4}^{(2)} \\ &= a_{n-2}^{(1)} - 2a_{n-3}^{(1)} + a_{n-4}^{(1)} \\ &= a_{n-1} - 3a_{n-2} + 3a_{n-3} - a_{n-4}. \end{aligned}$$

   Since the sequence given stabilises at layer 3, we have $a_{n-4}^{(3)} = a_{n-3}^{(3)}$. Writing this equality out and rearranging gives

$$\begin{aligned} a_{n-1} - 3a_{n-2} + 3a_{n-3} - a_{n-4} &= a_n - 3a_{n-1} + 3a_{n-2} - a_{n-3} \\ \Rightarrow \quad a_n &= 4a_{n-1} - 6a_{n-2} + 4a_{n-3} - a_{n-4}. \end{aligned}$$

   This calculation proves that for any sequence that stabilises at layer 3 (not just the one given in the question), each term is determined by the previous four terms. So, for example, we have

$$\begin{aligned} a_4 &= 4(43) - 6(13) + 4(5) - 7 = 107 \\ a_5 &= 4(107) - 6(43) + 4(13) - 5 = 217 \end{aligned}$$

   and so on. At this point, you could write a compute program or use a spreadsheet to compute a_{2026}. We're going to do something a little more human!

   Since the rest of the sequence is determined by a_0, a_1, a_2, and a_3, if we can find another sequence that stabilises at layer 3 with the same first four values, it must be this sequence! The question is how we find such a sequence. Thankfully, the previous question gives us a way to find it.

   From Question 3, if a sequence $b_0, b_1, b_2, \ldots$ is defined by $b_n = An^3 + Bn^2 + Cn + D$ for constants A, B, C, D with $A \neq 0$, then the sequence stabilises at layer 3. Let's see if we can find such constants so that $b_0 = 7$, $b_1 = 5$, $b_2 = 13$, and $b_3 = 43$.

   Supposing such constants existed, they would have to satisfy the following system of simultaneous equations:

$$\begin{aligned} b_0 = 7 &= A(0)^3 + B(0)^2 + C(0) + D \\ b_1 = 5 &= A(1)^3 + B(1)^2 + C(1) + D \\ b_2 = 13 &= A(2)^3 + B(2)^2 + C(2) + D \\ b_3 = 43 &= A(3)^3 + B(3)^2 + C(3) + D \end{aligned}$$

which after some simplification is equivalent to

$$\begin{aligned} D &= 7 \\ A + B + C + D &= 5 \\ 8A + 4B + 2C + D &= 13 \\ 27A + 9B + 3C + D &= 43. \end{aligned}$$

Subtracting the first equation from each of the other three and rearranging gives

$$\begin{aligned} C &= -2 - A - B \\ 8A + 4B + 2C &= 6 \\ 27A + 9B + 3C &= 36. \end{aligned}$$

Substituting the first into the other two, rearranging, and simplifying gives

$$\begin{aligned} 3A + B &= 5 \\ 4A + B &= 7 \end{aligned}$$

Subtracting the first equation from the second gives $A = 2$. Solving for the remaining variables gives $B = -1$ and $C = -3$.

Putting everything together, we must have that for all $n \geq 0$, $a_n = 2n^3 - n^2 - 3n + 7$. Substituting in $n = 2026$ gives $a_{2026} = 16\,628\,036\,405$.

Proofs of Facts 1 and 2

To keep things neat and tidy, we will declare that the polynomial $P(n) = 0$ has degree -1, and that non-zero constant polynomials have degree 0. You may have come across the convention that $P(n) = 0$ has degree $-\infty$, which would work equally as well. We will stick to the degree being -1.

For Fact 1, we will perform what is called a *proof by induction*.

Notice that the statement we wish to prove is true for $d = 1$ since $(n+1)^1 = n^1 + 1n^0 + 0$. We now assume that the statement is true for all integers d satisfying $1 \leq d \leq k$, for some positive integer k. The goal now is to show that the assumption implies that the statement is true for $k + 1$.

By our assumption, $(n+1)^k = n^k + kn^{k-1} + P(n)$ where $P(n)$ has degree at most $k - 2$. Then

$$\begin{aligned} (n+1)^{k+1} &= (n+1)(n+1)^k \\ &= (n+1)(n^k + kn^{k-1} + P(n)) \\ &= n^{k+1} + (k+1)n^k + kn^{k-1} + P(n) + nP(n). \end{aligned}$$

The polynomial $nP(n)$ has degree one more than that of $P(n)$. With a bit of thought, see if you can convince yourself that the degree of the sum of two polynomials cannot be larger than both degrees of the original polynomials. Therefore $Q(n) = kn^{k-1} + P(n) + nP(n)$ is a polynomial of degree at most $k - 1$. This proves the desired statement for $k + 1$.

So, we know the statement is true for $d = 1$, and therefore it's true for $d = 2$. Since it's true for $d = 1$ and $d = 2$, we proved that it must be true for $d = 3$. Continuing like this, we can conclude that for all integers $d \geq 1$, $(n+1)^d = dn^{d-1} + P(n)$ where $P(n)$ has degree at most $d - 2$.

For Fact 2, we will rely on Fact 1. We are given that $P(n)$ has degree d so we can write

$$P(n) = C_d n^d + C_{d-1} n^{d-1} + \cdots + C_1 n + C_0$$

where $C_0, C_1, \ldots, C_d$ are all constants, and $C_d \neq 0$. Then

$$P(n+1) = C_d (n+1)^d + C_{d-1} (n+1)^{d-1} + \cdots + C_1 (n+1) + C_0.$$

Applying Fact 1 to expand out $P(n+1)$ allows us to conclude that $P(n+1)$ has degree d. Therefore $P(n+1) - P(n)$ has degree at most d. In order to prove Fact 2, we need to show that the coefficient in front of the n^d term is zero. To that end, let's use Fact 1 to expand out $P(n+1) - P(n)$ a little. We have

$$P(n+1) - P(n) = C_d (n^d + dn^{d-1}) - C_d n^d + Q(n) = dC_d n^{d-1} + Q(n)$$

where $Q(n)$ is a polynomial of degree at most $d-1$. Therefore $P(n+1) - P(n)$ has degree at most $d-1$, completing the proof.

Problem of the Month

Problem 6: Cobbling cards

March 2026

The card game Cobble (not to be confused with the popular card game Dobble, also known as Spot It) is played with a special deck consisting of finitely many cards, each containing finitely many symbols. A Cobble deck satisfies the following properties:

(i) Each symbol appears at most once on each card.

(ii) Each pair of cards has exactly one symbol in common.

(iii) For any pair of symbols, there is exactly one card on which both symbols appear.

(iv) In the deck, there is some set of four symbols with the property that no three of them appear on the same card.

We denote each card by square braces, with the symbols listed inside. For example, $[A, B, D]$ denotes the card that contains the symbols A, B, and D. The collection of three cards

$$[A, B], [A, C], [B, C]$$

satisfies Properties (i), (ii), and (iii), but not Property (iv). Therefore, it is *not* a Cobble deck.

1. Construct a Cobble deck with seven cards using the seven symbols $\{A, B, C, D, E, F, G\}$.
2. Prove that there does not exist a Cobble deck with fewer than seven cards.
3. Show that in a Cobble deck, any two cards must each contain the same number of symbols. Conclude that each cord in a Cobble deck contains the same number of symbols.
4. Show that in a Cobble deck, for any two distinct symbols, they must appear on the same number of cards, and that number is the same as the number from Question 3. Conclude that each symbol in a Cobble deck appears on the same number of cards.
5. Prove that you cannot have a Cobble deck with 2026 cards.

Challenge. Construct a Cobble deck with 157 cards, or prove that you cannot do so.

Problem of the Month

Problem 6: Cobbling cards

March 2026

Hint

1. Property (iv) tells you that there must be at least four symbols. Let A, B, C, and D be four symbols satisfying that no three of them lie on the same card. Property (ii) tells you that each pair of these four symbols must appear on a distinct card. Start with these cards and see if you can build the deck from there, adding new symbols and new cards as necessary to satisfy the four properties of a Cobble deck.
2. As in the hint for Question 1, each Cobble deck must have a distinct card for each pair of the four symbols satisfying Property (iv). Start with those cards and try to build a Cobble deck without getting to seven cards. What goes wrong?
3. Start by proving that for any two cards in a Cobble deck, there is a symbol that does not appear on either card. Then see if you can use that symbol to create a kind of dictionary between the symbols on one of the cards and the symbols on the other card.
4. Cobble decks have a feature that you can change statements about cards into statements about symbols. See if you can first prove the counterpart to Property (iv): In a Cobble deck, there are four cards with the property that no three of them contain the same symbol. Once you have this, imitate your solution from Question 3.
5. Suppose each card has n symbols, and each symbol appears on n cards. Try to count the number of cards in the Cobble deck in terms of n.

Challenge. This is an open problem. I have no hints to give.

Problem of the Month

Solution to Problem 6: Cobbling cards

March 2026

1. Here is such a Cobble deck:

$$[A, B, E], [A, C, F], [A, D, G], [B, C, G], [B, D, F], [C, D, E], [E, F, G].$$

You should check that it satisfies the four properties from the definition given the problem statement. There are many other ways this could be done, but they all differ from this one by permuting the letters and permuting the cards.

To see how you could have constructed the deck, read through the solution to Question 2 including the note at the end.

2. Suppose A, B, C, and D are four symbols satisfying Property (iv). Then Properties (iii) and (iv) together tell us that each pair of these four symbols appears on a distinct card. This is because if two pairs appeared on the same card, we would have three of the four symbols appearing on the same card, contradicting Property (iv).

There are six distinct pairs you can create from the four symbols A, B, C, and D, and each needs to be on a distinct card. So, the six cards must look like

$$K_1 = [A, B, \ldots] \quad K_2 = [A, C, \ldots] \quad K_3 = [A, D, \ldots]$$
$$K_4 = [B, C, \ldots] \quad K_5 = [B, D, \ldots] \quad K_6 = [C, D, \ldots].$$

We have argued that there must be at least six cards in a Cobble deck, so to complete the question we must show that you cannot add symbols to these six cards to create a Cobble deck.

So far, this collection of cards satisfies Properties (i), (iii), and (iv), but not (ii). Currently, K_1 and K_6 do not have a symbol in common, K_2 and K_5 do not have a symbol in common, and K_3 and K_4 do not have a symbol in common.

Let's first look at K_1 and K_6. We cannot add C or D to K_1, since then A, B, C, and D would no longer satisfy Property (iv). Similarly, we cannot add A or B to K_6. Therefore, we need to introduce a new symbol to both K_1 and K_6. Call this new symbol E. The six cards must therefore look like this:

$$K_1 = [A, B, E, \ldots] \quad K_2 = [A, C, \ldots] \quad K_3 = [A, D, \ldots]$$
$$K_4 = [B, C, \ldots] \quad K_5 = [B, D, \ldots] \quad K_6 = [C, D, E, \ldots].$$

Let's now focus on K_2 and K_5. By a similar argument as we made for K_1 and K_6, we cannot add A, B, C, or D to either K_2 or K_5 to make the two cards contain a unique symbol in common. Furthermore, we cannot add E to both K_2 and K_5 because then K_2 and K_1 would share more than one symbol (and so would K_5 and K_6, K_2 and K_6, and K_1 and K_5).

We are therefore forced to introduce another symbol F to both K_2 and K_5.

A similar argument can be made for K_3 and K_4, whose conclusion is that yet another symbol G must be introduced to both cards.

Therefore, assuming these six cards form a Cobble deck, they must look like this:

$$K_1 = [A, B, E, \ldots] \quad K_2 = [A, C, F, \ldots] \quad K_3 = [A, D, G, \ldots]$$
$$K_4 = [B, C, G, \ldots] \quad K_5 = [B, D, F, \ldots] \quad K_6 = [C, D, E, \ldots].$$

These six cards now satisfy Properties (i), (ii), and (iv). However, (iii) is not satisfied since E and F (for example) do not appear together on any card.

The goal now is to force E and F to appear together on a unique card. Let's try to do this for each card one by one.

K_1: Introducing an F to K_1 would mean K_1 and K_2 share more than one symbol, so we cannot do this.

K_2: Adding E to K_2 means K_1 and K_2 share two symbols, an unacceptable state of affairs.

K_3: Putting both E and F on K_3 would force K_2 and K_3 to share A and F, which rules this possibility out.

K_4: Like the previous case, adding E and F to K_4 implies K_4 and K_5 share two symbols.

K_5: Placing E on K_5 is also not possible since K_5 and K_6 would then share two symbols.

K_6: Adding an F to K_6 forces K_5 and K_6 to have two symbols in common, which is simply not an option.

There is no path forward without introducing another card, and therefore there is no Cobble deck with six cards.

Note: We can remedy the situation by introducing a seventh card $[E, F, G]$, which results in the Cobble deck from the solution to Question 1.

3. We'll first prove a helpful result (which we will call a lemma, a word used in mathematics for an intermediary result used to prove a more desirable result).

Lemma: For any two cards in a Cobble deck, there is a symbol that is not on either card.

Proof. This proof will be a little sneaky. Our strategy will be to assume there are two cards that contain all the symbols that appear in the deck, and arrive at a contradiction.

Assume that K_1 and K_2 contain all the symbols in the Cobble deck. By Property (iv), there are four symbols so that no three of them appear on the same card. Therefore, two of them must appear on K_1 and two must appear on K_2. Let A and B be the two symbols appearing on K_1, and let C and D be the two symbols appearing on K_2. Note that none of A, B, C, or D appear on both K_1 and K_2 since then three of them would appear on one of the cards.

Let L_1 be the unique card containing A and C, and let L_2 be the unique card containing B and D. Note that L_1, L_2, K_1, and K_2 must be four distinct cards.

Let E be the unique symbol appearing on both L_1 and L_2. Note that E is distinct from A and B since A is not on L_2 and B is not on L_1 (can you see why?). The goal is to show that E cannot appear on K_1 or K_2, which will contradict our original assumption and complete the proof.

If E is on K_1, then E and A are both on L_1 and K_1, which cannot happen. If E is on K_2, then E and B are both on L_2 and K_2, which is impossible. Therefore, E is not on K_1 or K_2, completing the proof. □

Excellent! Let's now use the Lemma to give a solution to the original question. Let K_1 and K_2 be two distinct cards. Let P be a symbol not contained in either K_1 and K_2, which much exist by the Lemma. Suppose $K_1 = [A_1, A_2, \ldots, A_n]$. For each i between 1 and n, let L_i be the unique card containing A_i and P. Let B_i be the unique symbol contained in both L_i and K_2.

We want to show that $K_2 = [B_1, B_2, \ldots, B_n]$. The first thing is to show that each of the B_i are distinct. Suppose not, and suppose that $B_i = B_j$ for some $i \neq j$. Then B_i would be on both L_i and L_j. Since P is the unique symbol on both L_i and L_j, this would mean that $B_i = P$. However, P is not on K_2, a contradiction. Therefore, the symbols $B_1, B_2, \ldots, B_n$ are all distinct.

We must now show that there are no other symbols on K_2. To that end, suppose B is a symbol on K_2, and let L be the unique card containing B and P. Now, L and K_1 share a symbol. Since $K_1 = [A_1, A_2, \ldots, A_n]$, it must be the case that there is a unique t between 1 and n so that A_t is on both L and K_1. Since L contains A_t and P, it must be that $L = L_t$. Since B_t is the unique symbol on both L_t and K_2, and since B is contained on both L and K_2, we are forced to conclude that $B = B_t$.

We now have that $K_2 = [B_1, B_2, \ldots, B_n]$. Therefore, if a card contains n symbols, then every other card must also contain n symbols.

4. One of the (many) amazing things about Cobble decks is that roughly, you can change the roles of cards and symbols and prove similar statements. For example, the result we will prove in this question is the counterpart to the one in the previous question.

   To begin this question, we will first prove the counterpart of Property (iv), which we will call Property (v).

   Property (v): In a Cobble deck, there are four cards so that no three of them contain the same symbol.

   Proof. Let A, B, C, and D be the four symbols satisfying Property (iv) for the Cobble deck. Let K_1, K_2, K_3, and K_4 be the unique cards that contain A and B, B and C, C and D, and D and A respectively. The claim is that these four cards satisfy the property that no three of them contain the same symbol.

   The unique symbol common to K_1 and K_2 is B, the unique symbol common to K_2 and K_3 is C, the unique symbol common to K_3 and K_4 is D, and the unique symbol common to K_4 and K_1 is A.

   Since K_2 contains C, K_1 contains A, and the unique symbol common to K_1 and K_2 is B, K_1 does not contain C and K_2 does not contain A. Similarly,

   - K_2 does not contain D and K_3 does not contain B,

- K_3 does not contain A and K_4 does not contain C, and
- K_4 does not contain B and K_1 does not contain D.

Since K_3 does not contain the unique symbol common to K_1 and K_2 (which is B), there is no symbol that appears on K_1, K_2, and K_3. Since K_4 also does not contain B, there is no symbol appearing on the three cards K_1, K_2, and K_4.

Similarly, K_1 and K_2 do not contain the unique symbol common to K_3 and K_4 (which is D), so there is no symbol that appears on all three cards K_1, K_3, K_4, as well as K_2, K_3, K_4. This checks every possibility of three cards from the set K_1, K_2, K_3, K_4, and these four cards satisfy that no three of them contain the same symbol. □

Now, Properties (ii) and (iii) are counterparts of each other, and Properties (iv) and (v) are counterparts of each other. To run the argument from the previous question, we need a counterpart to the lemma from the previous question. While reading the proof, notice that the proof is the same as that of the Lemma in the previous question, but with the roles of the symbols and cards switched.

Lemma: For any two symbols in a Cobble deck, there is a card that does not contain either of them.

Proof. Let A and B be two symbols, and assume (towards a contradiction) that every card contains A or B (or both). By Property (v), there are four cards, no three of which contain the same symbol. Then two of these cards must contain A and not B, and the other two must contain B and not A. Let K_1 and K_2 be the cards containing A, and let K_3 and K_4 be the cards containing B.

Let C be the unique symbol appearing on K_1 and K_3, and let D be the unique symbol on K_2 and K_4. Let K be the unique card that contains C and D. To complete the proof of the lemma, it is enough to show that K does not contain A or B.

If K contains A, then K and K_1 contain both A and C, so they must be the same card. Also, K and K_2 both contain A and D, so they must also be the same card. But K_1 and K_2 are distinct cards, so this cannot happen and K cannot contain A. A similar argument shows that K cannot contain B, completing the proof of the lemma. □

Great, now everything is in place to run the same argument as in the previous question, but with the roles of the symbols and cards exchanged.

Let A and B be two distinct symbols. Let K be a card not containing A or B, whose existence is guaranteed by the Lemma. Let $K_1, K_2, \ldots, K_n$ be the cards containing A. For each integer i satisfying $1 \leq i \leq n$, let A_i be the unique symbol on K_i and K, and let L_i be the unique card containing A_i and B.

It remains to show that $L_1, L_2, \ldots, L_n$ is the set of cards containing B. First we must show that if $i \neq j$, L_i and L_j are distinct cards. If they are the same card, then A_i and A_j must be the same symbol. This would imply K_i and K_j are the same card, since they both contain A_i and A (which are two distinct symbols since K contains A_i but not A). However, we assumed that if $i \neq j$, K_i and K_j are distinct cards. Therefore, L_i and L_j must be distinct.

Now, to show $L_1, L_2, \ldots, L_n$ is the complete set of cards containing B, suppose L is some card containing B. We want to show that L is the same card as L_i for some i.

Let C be the unique symbol on L and K. Since A is not on K, C and A are distinct. Therefore, there is a unique integer i satisfying $1 \leq i \leq n$ so that K_i contains C and A. Since C is on K_i and K, it must be that $C = A_i$. Then L contains A_i and B, and so $L = L_i$.

We have proved that if one symbol appears on exactly n cards, then so does any other symbol.

To complete the question, we need to show that the number of cards that contain a particular symbol is equal to the number of symbols on a particular card.

To do this, suppose A is a symbol and let K be a card not containing A. Suppose $K = [B_1, B_2, \ldots, B_n]$. We want to show that A is contained in exactly n cards.

For each integer i satisfying $1 \leq i \leq n$, let K_i be the unique card containing A and B_i. Since each of the B_i are distinct, each of the K_i are distinct. Conversely, suppose L is a card containing A. Let B_t be the unique symbol on L and K. Then L contains B_t and A, and so $L = K_t$. Therefore, the list of cards $K_1, K_2, \ldots, K_n$ is precisely the list of cards containing A, and A is contained in exactly n cards.

5. From the previous question, we know that in any Cobble deck, the number of symbols on every card is equal to the number of cards containing any particular symbol. Call this number n. Let's count how many cards are in such a Cobble deck, in terms of n.

   Let $K = [A_1, A_2, \ldots, A_n]$ be a card. By the previous question, each of the A_i are on exactly $n-1$ other cards. This gives $n(n-1)$ other cards in the deck. We claim that these $n(n-1)$ cards, along with K, form all the cards in the deck.

   To see that all these cards are distinct, let L_1 and L_2 be two of the $n(n-1)$ cards. By the way they are constructed, neither are equal to K. Let the unique symbol shared by L_1 and K be A_t, and let the unique symbol shared by L_2 and K be A_s. If $A_t = A_s$, then L_1 and L_2 are distinct by the way they were constructed. If $A_t \neq A_s$, then A_t is on L_1 and A_t is not on L_2, so L_1 and L_2 are distinct.

   To see that these cards form all the cards in the Cobble deck, suppose L is some other card. Then L and K share a unique symbol A_t. Therefore, L is one of the $n-1$ other cards containing A_t, so we have accounted for all the cards in the Cobble deck.

   In terms of n (and adding one for the card K), the total number of cards in the Cobble deck is $n(n-1)+1 = n^2 - n + 1$. So, if there was a Cobble deck with 2026 cards, there would have to be a positive integer n satisfying $n^2 - n + 1 = 2026$. However, there are no integer solutions to this equation (which can be checked by solving the quadratic in n with the quadratic formula). Therefore, there is no Cobble deck with 2026 cards.

Challenge. No solution is given to this, because I do not know of a solution. In fact, no one does. This is an open problem. It is equivalent to the existence of what's called a *finite projective plane of order* 12.

The solution to Question 5 tells us that the number of cards in a Cobble deck must be an integer of the form $n^2 - n + 1$, where n is a positive integer. In Questions 1 and 2 we showed that the smallest n for which there is a Cobble deck is $n = 3$. Cobble decks are known to exist when $n = p^k + 1$ where p is a prime number and k is a positive integer. It is conjectured that these are the only possible values of n for which a Cobble deck exists, but very little has been proven about the nonexistence of Cobble decks.

It is known that Cobble decks do not exist for $n = 7$ and $n = 11$, but that's it! The smallest number for which this question is unsettled is $n = 13$, which corresponds to a Cobble deck with $13^2 - 13 + 1 = 157$ cards.

The game of Dobble (also known as Spot It) is played with what is almost a Cobble deck. The deck consists of cards, each with 8 symbols, and *almost* with each symbol appearing on 8 cards. If a Dobble deck were a Cobble deck, there would be $8^2 - 8 + 1 = 57$ cards in the deck. Inexplicably, there are only 55 cards in a Dobble deck. Go figure!

Problem of the Month

Problem 7: Sneaky Values

April 2026

The denominations that make up the currency in Canada, ignoring those less than a dollar, are \$1, \$2, \$5, \$10, \$20, \$50, and \$100. Using these denominations, we can realise any integer dollar value. For example, to make \$45, we could use four \$10s and one \$5, or two \$20s and one \$5, or even forty-five \$1s. The way to realise \$45 that uses the fewest items (coins or notes) is with two \$20s and one \$5, which uses three items.

1. Describe, with justification, how to obtain \$107 in Canada using the least number of items.
2. In the utopian (and sadly, fictitious) country of Cemcalia, the currency has notes with denominations 1, 5, 10, 18, and 30. Describe, with justification, how to obtain 37 using the least number of notes.

In order to investigate general currency systems, we will first set some notation. A *denomination set* is a tuple $(d_1, d_2, \ldots, d_k)$ of positive integers satisfying $d_1 = 1$ and $d_i < d_{i+1}$ for all i. Given such a denomination set, a *realisation* of a value v (which must be a positive integer) is a k-tuple of non-negative integers $N = (n_1, n_2, \ldots, n_k)$ so that $n_1d_1 + n_2d_2 + \cdots + n_kd_k = v$. Denote the number of items used in the realisation N by $|N| = n_1 + n_2 + \cdots + n_k$. The *greedy realisation* of v (denoted $G(v)$) is obtained by taking the largest denominations possible until the value is reached.

For example, in Canada, the denomination set is the 7-tuple $(1, 2, 5, 10, 20, 50, 100)$. The greedy realisation of the value 45 is $G(45) = (0, 0, 1, 0, 2, 0, 0)$ and $|G(45)| = 1 + 2 = 3$. The value 45 is also realised by the 7-tuples $(0, 0, 1, 4, 0, 0, 0)$ and $(45, 0, 0, 0, 0, 0, 0)$ (among others).

It is not necessarily the case that the greedy realisation uses the fewest items! For a value v, define $E(v)$ to be the smallest possible number $|N|$ over all realisations N of v. For example, consider the denomination set $(1, 15, 20)$. Then $E(30) = 2$ and $|G(30)| = |(10, 0, 1)| = 11$. It is a consequence of the definition of $E(v)$ that $E(v) \leq |G(v)|$ for all values v. A value v for which $E(v) < |G(v)|$ is called a *sneaky value*.

3. Find infinitely many denomination sets $(1, d_2, d_3)$ with the property that
   (a) $d_3 + 2$ is the smallest sneaky value.
   (b) $d_2 + d_3 - 1$ is the smallest sneaky value.
4. Let $(d_1, d_2, d_3, \ldots, d_k)$ be a denomination set.
   (a) Show that for any value $v > d_k$, $|G(v - d_k)| + 1 = |G(v)|$.
   (b) For all values v and all denominations $d_i < v$, show that $E(v - d_i) + 1 \geq E(v)$. When is the inequality an equality?
   (c) Suppose there are no sneaky values v satisfying $d_3 + 1 < v < d_{k-1} + d_k$. Prove that there are no sneaky values at all!

5. Using your favourite programming language, write a program that decides whether or not a denomination set $(d_1, d_2, \ldots, d_k)$ admits a sneaky value.

Problem of the Month
Problem 7: Sneaky Values
April 2026

Hint

1. Use the largest denominations first.
2. Using the largest denominations first may have worked for Question 1, but it does not give the correct answer here.
3. First find the smallest sneaky values for the denomination sets $(1, 5, 8), (1, 10, 18), (1, 5, 6)$, and $(1, 10, 11)$. To prove that your candidate sneaky values are indeed the smallest, it may help to prove the following statement: For a denomination set $(d_1, d_2, \ldots, d_k)$, if $v < d_3 + 2$, then v is not a sneaky value.
4. (a) Suppose $G(v) = (n_1, n_2, \ldots, n_k)$. See if you can find a formula for each of the n_i. You may have to define such a formula recursively.
   (b) Given a realisation $(n_1, n_2, \ldots, n_k)$ of $v - d_i$, how can you construct a realisation of v?
   (c) The statement given in the hint for Question 3 will be helpful here, as well as the previous two parts of this question. If you are unfamiliar with a proof by induction, it will be helpful to learn about it!
5. Question 4(c) shows that what at first glance appears to be an infinite search, is actually a finite search!

Problem of the Month

Solution to Problem 7: Sneaky Values

April 2026

This month's Problem of the Month centres around a well-known problem in computer science and optimisation known as the *change-making problem*. The questions in the POTM are inspired by, and closely follow, the results and arguments in the 1994 theoretical computer science paper *Optimal bounds for the change-making problem*, by Dexter Kozen and Shmuel Zaks.

1. I claim that the least number of items needed is three, and that is obtained by using one \$2, one \$5, and one \$100. This collection of denominations is an example of obtaining \$107 using three items, so we need to rule out the possibility that it can be done with one or two items.

   One item is not possible since \$107 is not an available denomination.

   Since all denominations except for \$1 and \$2 are a multiple of five, we cannot obtain \$107 without using some \$1s or \$2s. None of two \$1s, two \$2s, or one \$1 and one \$2 amounts to \$107. Since \$106 is not a denomination in the Canadian currency, \$107 cannot be obtained from two items by using exactly one \$1. Since \$105 is not an available denomination, \$107 cannot be obtained from two items by using exactly one \$2.

   We have ruled out the possibility that \$107 can be obtained by using only two items.

2. Since 37 is not a denomination, it cannot be obtained with one note.

   Since 37 is odd, it cannot be obtained with two of the same note. The possible totals obtainable by taking two distinct notes are $6, 11, 19, 31, 15, 23, 35, 28, 40$, and 48. None of these are equal to 37 and so 37 cannot be obtained with two notes.

3. (a) Let $t > 2$ be an integer. I claim that for the denomination set $(1, t, 2t-2)$, the value $2t$ is the smallest sneaky value.

   To see this, first note that $G(2t) = (2, 0, 1)$ and so $|G(t)| = 3$. However, $(0, 2, 0)$ is a realisation of $2t$ using only two items. Therefore $|G(2t)| > E(2t)$ and $2t$ is indeed a sneaky value. We need to show now that if $v < 2t$, it is not a sneaky value. We will do this by proving something a little more general:

   Claim: For a denomination set $(d_1, d_2, \ldots, d_k)$, if $v < d_3 + 2$, then v is not a sneaky value.

   Proving the claim will prove that $2t$ is the smallest sneaky value for the denomination set $(1, t, 2t-2)$.

   Proof of the claim. Let's start from the largest values of v. Suppose $v = d_3 + 1$. If $d_4 = d_3 + 1$, then certainly $E(v) = |G(v)| = 1$ so v is not sneaky. On the other hand, if v is not in the denomination set, it cannot be obtained with one item, so $E(v) \geq 2$. Also, $G(v) = (1, 0, 1, 0, \ldots, 0)$ so it must be the case that $E(v) = 2 = |G(v)|$ and thus v is not a sneaky value.

If $v = d_3$, then certainly $E(v) = |G(v)| = 1$ and it is not a sneaky value.

If $v < d_3$, then only the denominations 1 and d_2 can be used in any realisation of v. If n is the number of d_2s used in a realisation N of v, then $N = (v - nd_2, n, 0, \ldots, 0)$ and $|N| = v + n(1 - d_2)$. Since $d_2 > 1$, we have $1 - d_2 < 0$. So, to minimise $|N|$ we must maximise n. To do this, let $n = \left\lfloor \frac{v}{d_2} \right\rfloor$, where $\left\lfloor \frac{v}{d_2} \right\rfloor$ is the floor of $\frac{v}{d_2}$ (that is, the greatest integer less than or equal to $\frac{v}{d_2}$). Then

$$E(v) = v + \left\lfloor \frac{v}{d_2} \right\rfloor (1 - d_2).$$

The greedy realisation is also obtained by maximising the number of d_2s used. More precisely,

$$G(v) = \left(v - \left\lfloor \frac{v}{d_2} \right\rfloor d_2, \left\lfloor \frac{v}{d_2} \right\rfloor, 0, \ldots, 0 \right).$$

Therefore, $|G(v)| = E(v) = v + \left\lfloor \frac{v}{d_2} \right\rfloor$ and v is not a sneaky value. This completes the proof of the claim, and thus the solution to the question.

(b) Let $t > 2$ be an integer. Then I claim that for the denomination set $(1, t, t+1)$, $2t$ is the smallest sneaky value. Let's start by checking that $2t$ is indeed a sneaky value. Since $2t$ is not a denomination, and since $(0, 2, 0)$ is a realisation of $2t$, we have $E(2t) = 2$. However, $|G(2t)| = |(t - 1, 0, 1)| = t > 2$ and so $|G(2t)| \neq E(2t)$. We must now show that if $v < 2t$ it is not a sneaky value.

The claim from the solution to the previous question shows that if $v < t + 3$, then v is not a sneaky value. Suppose now that $t + 3 \leq v < 2t$. Then we cannot have more than one of either t or $t+1$ in a realisation of v. Therefore, there are only three possible realisations of v: $N = (v, 0, 0)$, $M = (v - t, 1, 0)$, and the greedy realisation $G(v) = (v - t - 1, 0, 1)$. We have $|N| = v$, $|M| = v - t + 1$ and $|G(v)| = v - t$. Therefore $E(v) = |G(v)| = v - t$ and v is not a sneaky value.

4. (a) Let $G(v) = (n_1, n_2, \ldots, n_k)$. The intuition behind this result is that you can obtain the greedy realisation of v from that of $v - d_k$ by simply adding one more d_k. Equivalently, our intuition suggests that $G(v - d_k) = (n_1, n_2, \ldots, n_{k-1}, n_k - 1)$.

To show that this is true, we will explicitly write out a formula for $G(v) = (n_1, n_2, \ldots, n_k)$, defining each n_i recursively.

The greedy realisation is obtained by first making n_k as large as possible. To do this we set

$$n_k = \left\lfloor \frac{v}{d_k} \right\rfloor,$$

where $\lfloor \alpha \rfloor$ is the floor of α, which is the greatest integer less than or equal to α. So, we have n_k copies of the denomination d_k, which leaves us with $v_{k-1} = v - n_k d_k$ remaining to make up from the other denominations. We now go to the next-largest denomination, and repeat the process.

More explicitly, let

$$n_{k-1} = \left\lfloor \frac{v_{k-1}}{d_{k-1}} \right\rfloor.$$

Adding n_{k-1} copies of d_{k-1} to the realisation leaves $v_{k-2} = v_{k-1} - n_{k-1}d_{k-1}$. We can now continue in this manner. In general, for each integer i satisfying $1 \leq i < k$ define

$$v_{k-i} = v_{k-(i-1)} - n_{k-(i-1)}d_{k-(i-1)} \quad \text{and} \quad n_{k-i} = \left\lfloor \frac{v_{k-i}}{d_{k-i}} \right\rfloor.$$

Note that when $i = k-1$ we get $n_1 = v_1$, which is the number of 1s used in the greedy realisation.

With the n_i defined this way, the greedy realisation of v is $G(v) = (n_1, n_2, \ldots, n_k)$.

Now, let $v > d_k$ and let $w = v - d_k$. Let $G(w) = (m_1, m_2, \ldots, m_k)$. We have

$$m_k = \left\lfloor \frac{v - d_k}{d_k} \right\rfloor = \left\lfloor \frac{v}{d_k} - 1 \right\rfloor = \left\lfloor \frac{v}{d_k} \right\rfloor - 1 = n_k - 1.$$

Furthermore,

$$w_{k-1} = w - m_k d_k = v - d_k - (n_k - 1)d_k = v - n_k d_k = v_{k-1}.$$

Therefore, for each integer i satisfying $k > i \geq 1$ we have $n_{k-i} = m_{k-i}$. Putting all of this together we have that if $G(v) = (n_1, n_2, \ldots, n_k)$, then

$$G(v - d_k) = (n_1, n_2, \ldots, n_{k-1}, n_k - 1).$$

Therefore, $|G(v - d_k)| + 1 = |G(v)|$.

(b) Suppose $N = (n_1, n_2, \ldots, n_k)$ is a realisation of $v - d_i$ satisfying $|N| = E(v - d_i)$. Then $N' = (n_1, n_2, \ldots, d_{i-1}, d_i + 1, d_{i+1}, \ldots, d_k)$ is a realisation of v. Furthermore,

$$|N'| = |N| + 1 = E(v - d_i) + 1.$$

By the definition of $E(v)$, we have that $E(v) \leq |M|$ for all realisations M of v. Therefore, $E(v) \leq E(v - d_i) + 1$.

Now to address the question of when $E(v) = E(v - d_i) + 1$. Let's assume the equality holds and see what comes of it.

Let $M = (m_1, m_2, \ldots, m_k)$ be a realisation of $v - d_i$ satisfying $|M| = E(v - d_i)$. Then $M' = (m_1, m_2, \ldots, m_{i-1}, m_i + 1, m_{i+1}, \ldots, m_k)$ is a realisation of v satisfying $|M'| = E(v - d_i) + 1 = E(v)$. Therefore, if $E(v) = E(v - d_i) + 1$, then there exists a realisation $N = (n_1, n_2, \ldots, n_k)$ of v such that $n_i > 0$ (that is, the denomination d_i is used) and $|N| = E(v)$.

Let's see if the converse holds. Assume now that $N = (n_1, n_2, \ldots, n_k)$ is a realisation of v so that $|N| = E(v)$ and that $n_i > 0$. Then $N' = (n_1, n_2, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k)$ is a realisation of $v - d_i$ satisfying $|N'| = |N| - 1 = E(v) - 1$. However, we know from the inequality in the first part of this question that $E(v) - 1 \geq E(v - d_i)$. We also know by the definition of $E(v - d_i)$ that $|N'| \geq E(v - d_i)$. Putting all of this together we have

$$E(v - d_i) \geq E(v) - 1 = |N| - 1 = |N'| \geq E(v - d_i).$$

The only way this can happen is if $E(v - d_i) = E(v) - 1$.

We have proved the following statement. Suppose $d_i < v$. Then $E(v) = E(v - d_i) + 1$ exactly when there exists a realisation $N = (n_1, n_2, \ldots, n_k)$ of v such that $|N| = E(v)$ and $n_i > 0$.

(c) First recall the claim from the solution to Question 3(a), which says that if $v < d_3+2$, then v is not a sneaky value. Combining that claim with the assumptions given in the question, we have that for all $v < d_{k-1} + d_k$, v is not a sneaky value.

We will now proceed using a technique known as induction. Here's the idea. To prove that some $v \geq d_{k-1}+d_k$ is not a sneaky value, we will assume that for all values $w < v$, w is not a sneaky value. From that assumption, we will try to prove that v is not a sneaky value.

This technique actually proves infinitely many statements at once, and here's why it works. From what we've deduced so far, we know that for all $w < d_{k-1}+d_k$, w is not a sneaky value. So, assuming we can prove what we want to, we will then be able to deduce that $v = d_{k-1} + d_k$ is not a sneaky value. This result in turn will imply that $v+1$ is not a sneaky value, which then implies $v+2$ is not a sneaky value, and so on forever! The fact that this works is actually a fundamental defining property of the natural numbers. With that in mind, let's do it!

Let $v \geq d_{k-1} + d_k$ and assume that for all $w < v$, $|G(w)| = E(w)$ (that is, w is not a sneaky value). Now suppose that $N = (n_1, \ldots, n_k)$ is a realisation of v satisfying $|N| = E(v)$. Choose an n_i so that $n_i > 0$ (which must exist since $v > 0$).

If $n_i = n_k$, then

$$|G(v)| = |G(v - d_k)| + 1 = E(v - d_k) + 1 = E(v)$$

where the first equality is by 4(a), the second equality is by our assumption that $v-d_k$ is not a sneaky value, and the third equality is from the solution to 4(b). Therefore, v is not a sneaky value.

If $n_i \neq n_k$, then

$$\begin{aligned}
|G(v)| &= |G(v - d_k)| + 1 && \text{by 4(a)} \\
&= E(v - d_k) + 1 && \text{by our assumption} \\
&\leq E(v - d_k - d_i) + 2 && \text{by 4(b)} \\
&\leq |G(v - d_k - d_i)| + 2 && \\
&= |G(v - d_i)| + 1 && \text{by 4(a)} \\
&= E(v - d_i) + 1 && \text{by our assumption} \\
&= E(v) && \text{by the solution to 4(b)} \\
&\leq |G(v)|. &&
\end{aligned}$$

The important part of this chain of equalities and inequalities is that

$$|G(v)| \leq E(v) \leq |G(v)|,$$

which can only happen if $|G(v)| = E(v)$. Therefore, v is not a sneaky value, completing the proof.

5. Code will not be explicitly produced here, but an algorithm will be described that we know works due to the previous questions.

Question 4(c) and the claim in the solution to Question 3(a) shows us that if a sneaky value exists, then the smallest sneaky value v satisfies $d_3 + 1 < v < d_{k-1} + d_k$.

Therefore we only have to check finitely many values of v and decide whether or not v is a sneaky value. This is possible to do on a computer since if $(n_1, n_2, \ldots, n_k)$ is a realisation of v, we must have

$$n_i \leq \left\lfloor \frac{v}{d_i} \right\rfloor$$

for all i. Therefore there are finitely many possible realisations of v. The solution to 4(a) gave an explicit algorithm to compute the greedy realisation of v, and so we can check each realisation N of v and determine whether or not $|N| < |G(v)|$.

All of these checks can be done in a finite number of steps, and can therefore be programmed into a computer (although this can certainly be implemented more efficiently).

If there is a value v in the finite range $d_3 + 1 < v < d_{k-1} + d_k$ and a realisation N of v satisfying $|N| < |G(v)|$, then the denomination set $(d_1, d_2, \ldots, d_k)$ admits a sneaky value (and one of the sneaky values is v). If for every v in the range $d_3 + 1 < v < d_{k-1} + d_k$, all realisations N of v satisfy $|N| \geq |G(v)|$, then the denomination set does not admit a sneaky value.

Can you come up with a more efficient algorithm than the one described here, and prove that it works?

Problem of the Month

Problem 8: Revolutionary counting

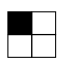
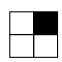
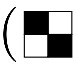
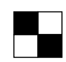
May 2026

This Problem of the Month is inspired by Question 24 of the Team Problems from the CEMC's 2026 Canadian Team Mathematics Contest:

> In a 4×4 grid consisting of 16 unit squares, 4 squares are coloured red, while the other 12 are coloured white. Two colourings are said to be equivalent if one can be obtained from the other by doing a sequence of $90°$ rotations. How many inequivalent colourings are there?

Try the problem as a warm up! The following problems will investigate counting problems of the form "in how many inequivalent ways can you colour something where two colourings are equivalent if one can be obtained from the other by a rotation?"

1. Consider a 2×2 grid of four unit squares, where each square is coloured either black or white. Let r_1, r_2, r_3, and r_0 denote the rotations of the grid by $90°$ clockwise, $180°$ clockwise, $270°$ clockwise, and $0°$ respectively. View these four rotations as functions that take as an input a colouring of the grid, and give as an output a colouring. For example,

   $r_1($  $) =$ , $\quad r_2($  $) =$ ,

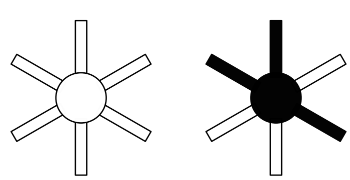
   and $r_0(c) = c$ for all colourings c. Two colourings c and d are equivalent if there is a rotation r so that $r(c) = d$.

   (a) How many inequivalent colourings of the 2×2 grid exist?

   (b) For each rotation r, let $\text{fix}(r)$ be the number of colourings c satisfying $r(c) = c$. Compute $\text{fix}(r_0) + \text{fix}(r_1) + \text{fix}(r_2) + \text{fix}(r_3)$.

   (c) Compare your answers to the previous two parts.

2. Consider a windmill with six identical blades evenly spaced around a central circle. The central circle, and each of the blades, are to be coloured either black or white. Let r_0, r_1, r_2, r_3, r_4, and r_5 denote the rotations of the windmill by $0°, 60°, 120°, 180°, 240°$, and $300°$ clockwise, respectively. Two colourings c and d are equivalent if there is a rotation r such that $r(c) = d$. The image below shows two inequivalent colourings of the windmill.

   (a) How many inequivalent colourings of the windmill are there?

   (b) For each rotation r let $\text{fix}(r)$ denote the number of colourings c of the windmill satisfying $r(c) = c$. Compute $\text{fix}(r_0) + \text{fix}(r_1) + \text{fix}(r_2) + \text{fix}(r_3) + \text{fix}(r_4) + \text{fix}(r_5)$.

(c) Compare your answers to the previous two parts.

3. Now for a more general approach! Suppose we have some object and k rotations $r_0, r_1, \ldots, r_{k-1}$ we can perform on the object, where r_z is a rotation by $\frac{360z}{k}$ degrees clockwise. Assume that the object can be coloured according to some rules, and consider the collection of all possible colourings of the object according to the rules. In Question 1 for example, the object is the 2×2 grid, $k = 4$ since there are four rotations, and there are $2^4 = 16$ possible colourings of the grid where each square is either black or white. Two colourings c and d are *equivalent* if there is a rotation r so that $r(c) = d$. Let N be the number of inequivalent colourings of the object.

   (a) Fix a colouring c. Let $E(c)$ be the number of colourings (including c itself) that are equivalent to c. Let $S(c)$ be the number of rotations satisfying $r(c) = c$. Show that $E(c)S(c) = k$.

   (b) A *stable pair* is a pair (r, c) where r is a rotation, c is a colouring, and $r(c) = c$. Show that the number of stable pairs is equal to kN.

   (c) For a rotation r, let $\text{fix}(r)$ denote the number of colourings c satisfying $r(c) = c$. Show that the number of stable pairs is equal to $\text{fix}(r_0) + \text{fix}(r_1) + \cdots + \text{fix}(r_{k-1})$.

4. Consider the 4×4 grid of 16 unit squares given at the beginning of this document. Let r_0, r_1, r_2, and r_3 be the rotations by $0°$, $90°$, $180°$, and $270°$ clockwise, respectively. By computing $\text{fix}(r_0) + \text{fix}(r_1) + \text{fix}(r_2) + \text{fix}(r_3)$, solve the problem at the beginning of this document.

5. Let p be a prime. Consider a windmill with p identical blades evenly spaced around a central circle. The central circle, and each of the blades, are to be coloured either black or white. Two colourings are considered equivalent if you can rotate one into the other. How many inequivalent colourings of the windmill are there?

Problem of the Month

Problem 8: Revolutionary counting

May 2026

Hint

1. (a) Draw out all 16 possible colourings and group them into collections of equivalent colourings. Count the number of groups you have.

   (b) The rotation that does nothing always fixes every colouring. For the other rotations, draw out the 16 possible colourings and rotate them to figure out if the colouring changes under a particular rotation.

   (c) The answer to part (b) is a multiple of the answer to part (a). What is that multiple?

2. (a) Try organising your count by counting the number of inequivalent colourings of the windmill with 0 black blades. Then with 1 black blade. Then with 2, and then with 3 black blades. At this point, you've already secretly counted the number of inequivalent colourings of the windmill with 4, 5, and 6 black blades.

   (b) Fix some rotation, and suppose that the rotation takes some blade to another blade. In order for a colouring to be fixed by the rotation, those two blades must be the same colour.

   (c) The answer to part (b) is a multiple of the answer to part (a). What is that multiple?

3. (a) Since we are thinking of rotations as functions, we can take the composition of two rotations and get another rotation. Suppose $E(c) = t$ and $S(c) = m$. The goal is to show $sm = k$. Denote the t distinct equivalent colourings by $q_0(c), q_1(c), \ldots, q_{t-1}(c)$ for some rotations $q_0, q_1, \ldots, q_{t-1}$. Let $s_0, s_1, \ldots, s_{m-1}$ be the rotations satisfying $s_j(c) = c$. Consider all compositions $q_i \circ s_j$, of which there are tm. Try to show that every rotation can be uniquely written as $q_i \circ s_j$. It may help to prove (and use) the following fact: for any rotation r, there exists a rotation r' so that $r' \circ r = r_0$.

   (b) Fix a colouring c. How many stable pairs have c in the second coordinate? For the collection of all colourings d equivalent to some fixed colouring c, what is the sum of all the $S(d)$? Part (a) will come in handy for this question.

   (c) Fix a rotation r. How many stable pairs have r in the first coordinate?

4. Question 3 tells us that the number of inequivalent colourings of the grid is equal to

$$\frac{\text{fix}(r_0) + \text{fix}(r_1) + \text{fix}(r_2) + \text{fix}(r_3)}{4}.$$

5. First try to prove that $\text{fix}(r)$ is the same for all rotations other than r_0. Such a proof will rely on the fact that p is prime.

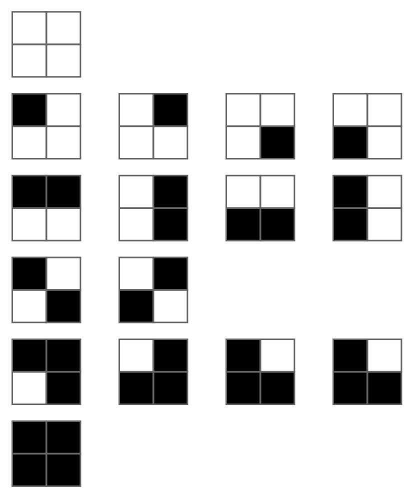
Problem of the Month

Solution to Problem 8: Revolutionary counting

May 2026

The counting technique developed in this Problem of the Month is often referred to as *Burnside enumeration* or *Burnside's lemma*. In today's mathematical landscape, it falls under the purview of *group theory* or *enumeration*.

1. (a) Below are the $2^4 = 16$ colourings of the 2×2 grid, arranged into rows. All colourings in the same row are equivalent.

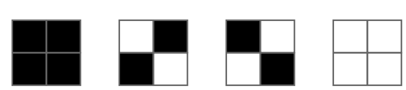


Since there are six rows, there are six inequivalent colourings.

(b) All 16 colourings satisfy $r_0(c) = c$, since r_0 doesn't do anything to the grid! So $\text{fix}(r_0) = 16$.

To calculate $\text{fix}(r_1)$, note that the colour or the top-left square must be the same as the colour of the top-right square since the colouring of the grid doesn't change after a rotation of 90° clockwise. Similarly, the colour of the top-right square must be the same as that of the bottom-right square, and the bottom-left square. Therefore the only two colourings c that satisfy $r_1(c) = c$ are the colourings with all four squares coloured the same colour. Therefore $\text{fix}(r_1) = 2$. A similar argument shows $\text{fix}(r_3) = 2$.

For a colouring to be fixed by r_2, the top-left and bottom-right squares must be the same colour, and the top-right and bottom-left squares must be the same colour. There are four such colourings shown here:



Therefore, $\text{fix}(r_2) = 4$.

Putting everything together we have

$$\text{fix}(r_0) + \text{fix}(r_1) + \text{fix}(r_2) + \text{fix}(r_3) = 16 + 2 + 4 + 2 = 24.$$

(c) If N is the number of inequivalent colourings, then

$$\text{fix}(r_0) + \text{fix}(r_1) + \text{fix}(r_2) + \text{fix}(r_3) = 4N.$$

Note that 4 is the number of possible rotations.

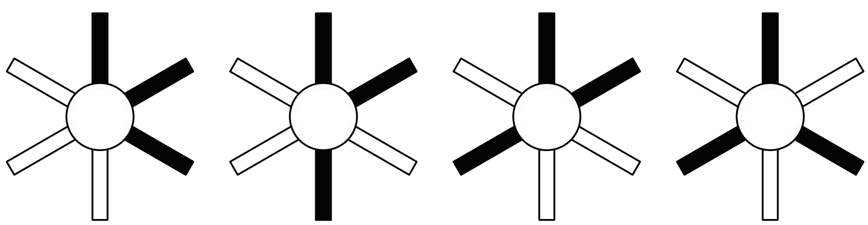
2. (a) We will first count the number of inequivalent colourings when the central circle is white, and our final answer will be double the result.

There is one colouring when all blades are black. There is one colouring when all blades are white.

There is six ways to colour the windmill with exactly one black blade, but they are all equivalent. The same holds for the number of colourings with exactly one white blade.

Suppose now that exactly two blades are black. They can either be adjacent, separated by one white blade, or separated by two white blades. Any two colourings with the same number of white blades separating the two black blades are equivalent. Therefore, there are three inequivalent colourings with two black blades. The same holds for the case when there are exactly two white blades.

When there are three black and three white blades, there are four inequivalent colourings as shown.



This gives a total of 14 inequivalent colourings when the central circle is white, and therefore a total of $2 \times 14 = 28$ inequivalent colourings of the windmill in total.

(b) There are 7 regions that can be coloured either black or white, and therefore 2^7 possible colourings of the windmill. All of these colourings are fixed by r_0, and therefore $\text{fix}(r_0) = 2^7$.

Starting from the top of the windmill and going clockwise, name the blades

$$b_1, b_2, b_3, b_4, b_5 \quad \text{and} \quad b_6.$$

Just like we think of the rotations as functions with inputs and outputs colourings of the windmill, we can similarly view rotations as functions with inputs and outputs the blades of the windmill. Note that $r_1(b_1) = b_2$, $r_1(b_2) = b_3$, $r_1(b_3) = b_4$, $r_1(b_4) = b_5$, and $r_1(b_5) = b_6$. Therefore, for a colouring to be fixed by r_1, the colour of b_1 should be the same as that of b_2, which should be the same as that of b_3, b_4, b_5, and b_6. Said a different way, all the blades must be the same colour! There are two choices for the colour of the central circle, and two choices for the colour of the blades. Therefore, $\text{fix}(r_1) = 4$. A similar argument shows that $\text{fix}(r_5) = 4$.

To compute $\text{fix}(r_2)$, observe that $r_2(b_1) = b_3$, $r_2(b_3) = b_5$, and $r_2(b_5) = b_1$. Therefore, b_1, b_3, and b_5 must all be the same colour for a colouring fixed by r_2. Similarly, since $r_2(b_2) = b_4$, $r_2(b_4) = b_6$, and $r_2(b_6) = b_2$, we must have that b_2, b_4, and b_6 must be the same colour. So, supposing a colouring c satisfies $r_2(c) = c$, there are two choices for the colour of the central circle, two choices for the colour of b_1 (which fixes the colour of b_3 and b_5), and two choices for the colour of b_2 (which fixes the colour of b_4 and b_6). Therefore, $\text{fix}(r_2) = 2^3 = 8$. A similar argument shows $\text{fix}(r_4) = 8$.

Now onto the rotation r_3. Observe that $r_3(b_1) = b_4$ and $r_3(b_4) = b_1$ and so b_1 and b_4 must have the same colour in a colouring fixed by r_3. Similarly, b_2 and b_5 must have the same colour, and b_3 and b_6 must have the same colour. So, a colouring of the windmill that is fixed by r_3 is determined by the colours of the central circle, b_1, b_2, and b_3. Each of these regions has two possible colours, so $\text{fix}(r_3) = 2^4 = 16$.

Organising all of this information gives

$$\text{fix}(r_0) + \text{fix}(r_1) + \cdots + \text{fix}(r_5) = 2^7 + 4 + 8 + 16 + 8 + 4 = 168.$$

(c) The answers to the previous two parts are 28 and 168. It turns out that $28 \times 6 = 168$, and 6 is the number of possible rotations.

3. (a) Suppose $E(c) = t$, and let the t distinct equivalent colourings be given by

$$q_0(c), q_1(c), q_2(c), \ldots, q_{t-1}(c),$$

where the q_i are distinct rotations with $q_0 = r_0$ (so $q_0(c) = c$). Let $S(c) = m$ and let $s_0, s_1, \ldots, s_{m-1}$ be the m distinct rotations satisfying $s_j(c) = c$, with $s_0 = r_0$.

For two rotations s and q, let $q \circ s$ denote the rotation obtained by performing s followed by q. Note that the composition of two rotations is another rotation.

Consider now all compositions of the form $q_i \circ s_j$. There are m choices for s_j and t choices for q_i, so there are mt such compositions. The goal is to show that every rotation is the same as exactly one of these compositions, and hence conclude that $k = mt$.

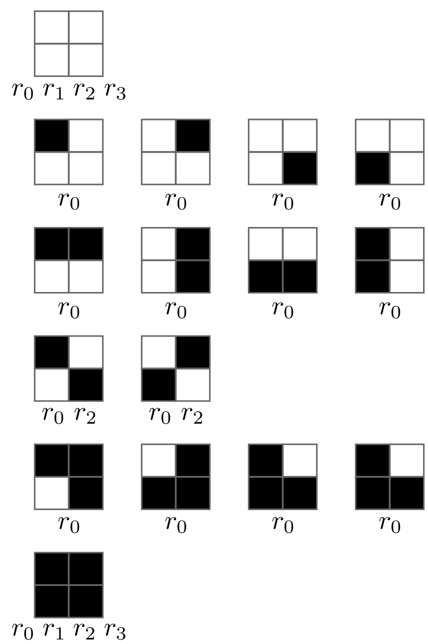
To that end, let $0 \le i_1, i_2 \le t-1$, $0 \le j_1, j_2 \le m-1$, and suppose $q_{i_1} \circ s_{j_1}$ and $q_{i_2} \circ s_{j_2}$ are the same rotation. Then $q_{i_1} \circ s_{j_1}(c) = q_{i_2} \circ s_{j_2}(c)$. Since each of the s_j fix c, as a consequence we get $q_{i_1}(c) = q_{i_2}(c)$. However, the q_i were defined so that distinct q_j give distinct colourings $q_j(c)$. So, the only way $q_{i_1}(c) = q_{i_2}(c)$ is if $q_{i_1} = q_{i_2}$. Denote the rotation q_{i_1} simply by q_i.

Recall that q_i is a rotation by $\frac{360z}{k}$ degrees clockwise for some integer z. Let q be the rotation by $\frac{360(k-z)}{k}$ degrees clockwise. Then $q \circ q_i$ is the rotation r_0 (the rotation that does nothing!). Our initial assumption is that $q_i \circ s_{j_1}$ is the same rotation as $q_i \circ s_{j_2}$. Composing both of these rotations with q gives that $q \circ q_i \circ s_{j_1}$ is the same rotation as $q \circ q_i \circ s_{j_2}$. However, $q \circ q_i \circ s_{j_1} = r_0 \circ s_{j_1} = s_{j_1}$ and similarly $q \circ q_i \circ s_{j_2} = s_{j_2}$. Therefore s_{j_1} and s_{j_2} are the same rotation. We can conclude that the collection of rotations $q_i \circ s_j$ where i ranges from 0 to $t-1$ and j ranges from 0 to $m-1$ is a collection of mt distinct rotations.

It remains to show that every rotation is of the form $q_i \circ s_j$ for some i and j. Let r be an arbitrary rotation. Then $r(c)$ is a colouring equivalent to c, and so there exists some i so that $q_i(c) = r(c)$. As we argued above, there is some rotation q so that $q \circ q_i = r_0$. Applying q to the colouring $q_i(c) = r(c)$ gives $q \circ r(c) = q \circ q_i(c) = r_0(c) = c$.

Therefore, $q \circ r$ is equal to some rotation s_j. Composing $q \circ r$ and s_j with q_i gives $q_i \circ s_j = q_i \circ q \circ r = r_0 \circ r = r$, completing the proof.

(b) Let's look more closely at the example from Question 1 to guide us in our solution. Here is a picture of all the colourings of the 2×2 grid, organised into rows of equivalent colourings. The rotations that fix each colouring appear below that colouring:



There are a few important things to notice here.

- If we count the number of rotations appearing in each row, it is always four (which is the value of k, the total number of rotations). This corresponds to there being four stable pairs containing the colourings in any row.
- The number of rotations appearing below a colouring c is the number of stable pairs containing c in the second coordinate, which is also the value of $S(c)$.
- The number of rotations below a colouring c is equal to four divided by the number of colourings in its row. This is a reflection of the fact from 3(a) that $E(c)S(c) = k$ (can you see why?).
- The total number of stable pairs is equal to the number of rotations that appear in the entire image. Since there are $k = 4$ rotations in each row, and $N = 6$ rows, the number of stable pairs is $kN = 24$.

These four points provide an outline of our solution to the general case. Here we go!

Fix some colouring c. The number of stable pairs with c in the second coordinate is equal to the number of rotations r satisfying $r(c) = c$. Therefore the number of stable pairs with c in the second coordinate is $S(c)$. If we sum up $S(c)$ over all colourings c we get the number of stable pairs.

Suppose that $E(c) = t$ and $c_1, c_2, \ldots, c_t$ are the t colourings equivalent to c (so in particular, one of the c_i is c). By 3(a), for each i we have $S(c_i) = \frac{k}{E(c_i)} = \frac{k}{t}$. Therefore,

$$S(c_1) + S(c_2) + \cdots + S(c_t) = \underbrace{\frac{k}{t} + \frac{k}{t} + \cdots + \frac{k}{t}}_{t \text{ times}} = k.$$

We have shown that if we sum up $S(c)$ over all colourings that are equivalent to a particular fixed colouring, we get k. Since there are N inequivalent colourings, summing up $S(c)$ over all colourings gives kN. Since the number of stable pairs is the sum over all colourings c of $S(c)$, we conclude that the number of stable pairs is equal to kN.

(c) If we fix a rotation r, the number of stable pairs with r in the first coordinate is the number of colourings c satisfying $r(c) = c$. This is precisely $\mathrm{fix}(r)$. Therefore, to count all stable pairs we can sum up $\mathrm{fix}(r)$ over all possible rotations. Said another way, the number of stable pairs is equal to $\mathrm{fix}(r_0) + \mathrm{fix}(r_1) + \cdots + \mathrm{fix}(r_{k-1})$.

The important thing to take away from Question 3 is that the quantities kN and

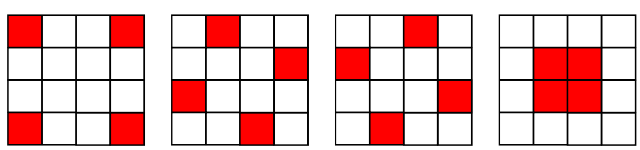
$$\mathrm{fix}(r_0) + \mathrm{fix}(r_1) + \cdots + \mathrm{fix}(r_{k-1})$$

both count the number of stable pairs, and are therefore equal!

4. The number of possible colourings of the grid with exactly four red squares is the binomial coefficient $\binom{16}{4} = \frac{16!}{(12!)(4!)} = 1820$. Since all colourings are fixed by r_0, $\mathrm{fix}(r_0) = 1820$.

Observe that r_1 moves the four squares in the top-left quarter of the grid to the top-right quarter. It moves the four squares in the top-right quarter to the bottom-right quarter, and it moves the four squares in the bottom-right quarter to the bottom-left quarter. Therefore, a colouring of the grid with four red squares that is fixed by r_1 must have exactly one red square in each of the four quarters of the grid. In fact, the colouring is entirely determined by which of the four squares in the top-left quarter is coloured red.

There are four possibilities for which square in the top-left quarter of the grid is coloured red, and therefore $\mathrm{fix}(r_1) = 4$. A similar argument shows $\mathrm{fix}(r_3) = 4$. The next image shows the four colourings of the grid fixed by r_1 (and r_3).



We can compute $\mathrm{fix}(r_2)$ in a similar way, except this time a colouring fixed by r_2 is determined by which two squares in the top half of the grid are coloured red. There are $\binom{8}{2} = 28$ ways to colour two of the eight squares in the top half of the grid red, which gives $\mathrm{fix}(r_2) = 28$.

From Question 3, we know that the number of inequivalent colourings of the grid is equal to

$$\frac{1}{4}\left(\text{fix}(r_0) + \text{fix}(r_1) + \text{fix}(r_2) + \text{fix}(r_3)\right) = \frac{1820 + 4 + 28 + 4}{4} = 464.$$

5. Let $r_0, r_1, \ldots, r_{p-1}$ be the p rotations of the windmill, where r_j is a rotation by $\frac{360j}{p}$ degrees clockwise. From Question 3 we know that the number of inequivalent colourings of the windmill is

$$\frac{1}{p}\left(\text{fix}(r_0) + \text{fix}(r_1) + \cdots + \text{fix}(r_{p-1})\right).$$

There are $p+1$ regions (including the central circle) that can either be coloured black or white. Therefore, there are 2^{p+1} possible colourings of the windmill, and $\text{fix}(r_0) = 2^{p+1}$.

Let r be any other rotation. Arrange the windmill so one of the blades is pointing straight up. Starting from the top and going clockwise, label the blades $b_1, b_2, \ldots, b_p$. For a positive integer t, denote by r^t the rotation obtained by composing r with itself t times. So, for example, $r_1^3 = r_1 \circ r_1 \circ r_1 = r_3$.

Now, consider the sequence of blades $b_1, r(b_1), r^2(b_1), r^3(b_1), \ldots$. Since there are only finitely many blades, there will be an appearance of at least one blade more than once. Suppose that the first time we get a repeated blade occurring in the sequence is at $r^t(b_1)$ and $r^{t+s}(b_1) = r^s(r^t(b_1))$. Since r^s is some rotation that fixes a blade, it must be that $r^s(b_i) = b_i$ for all the blades b_i. Furthermore, since this is the first time in the sequence a blade appears twice, we must have that for all blades b, $r^l(b) \neq b$ for any integer l satisfying $1 \leq l < s$.

Our goal is to now show that $s = p$. Since r is a rotation by $\frac{360j}{p}$ degrees clockwise (for some integer j), r^p is a rotation by $360j$ degrees clockwise. Since this is a multiple of $360°$, it must be the case that $r^p(b) = b$ for all blades b. Therefore, we have $1 < s \leq p$ (the first inequality is since $r \neq r_0$).

Suppose that $s < p$. Since p is prime, there is some remainder when you divide p by s. That is, there are integers q and m with $1 \leq m < s$ such that $p = qs + m$. For a blade b we have

$$b = r^p(b) = r^{qs+m}(b) = r^m\,\underbrace{(r^s(r^s(r^s(\cdots r^s}_{q\text{ times}}(b))))) = r^m(b).$$

This is a contradiction since $1 \leq m < s$ and so $r^m(b) \neq b$. We are forced to conclude that $s = p$.

Returning to how we defined s, we must have that the p blades $r^t(b_1), r^{t+1}(b_1), \ldots, r^{t+p-1}(b_1)$ are distinct, and thus every blade appears exactly once in the list of p blades. Therefore, any colouring of the windmill that is fixed by r must have every blade be the same colour! Therefore, for any colouring fixed by r, there are two choices for the colour of the central circle, and two choices for the colour of the blades. We therefore have that $\text{fix}(r) = 4$.

Finally, the number of inequivalent colourings of the windmill is

$$\frac{1}{p}\left(\text{fix}(r_0) + \text{fix}(r_1) + \cdots + \text{fix}(r_{p-1})\right) = \frac{2^{p+1} + 4(p-1)}{p}.$$