Canadian Mathematical Olympiad 2018

Official Solutions

1. Consider an arrangement of tokens in the plane, not necessarily at distinct points. We are allowed to apply a sequence of moves of the following kind: Select a pair of tokens at points A and B and move both of them to the midpoint of A and B.

   We say that an arrangement of n tokens is *collapsible* if it is possible to end up with all n tokens at the same point after a finite number of moves. Prove that every arrangement of n tokens is collapsible if and only if n is a power of 2.

   Solution. For a given positive integer n, consider an arrangement of n tokens in the plane, where the tokens are at points A_1, A_2, $\ldots$, A_n. Let G be the centroid of the n points, so as vectors (after an arbitrary choice of origin),

   $$\overrightarrow{G} = \frac{\overrightarrow{A}_1 + \overrightarrow{A}_2 + \cdots + \overrightarrow{A}_n}{n}.$$

   Note that any move leaves the centroid G unchanged. Therefore, if all the tokens are eventually moved to the same point, then this point must be G.

   First we prove that if $n = 2^k$ for some nonnegative integer k, then all n tokens can always be eventually moved to the same point. We shall use induction on k.

   The result clearly holds for $n = 2^0 = 1$. Assume that it holds when $n = 2^k$ for some nonnegative integer k. Consider a set of 2^{k+1} tokens at A_1, A_2, $\ldots$, $A_{2^{k+1}}$. Let M_i be the midpoint of A_{2i-1} and A_{2i} for $1 \le i \le 2^k$.

   First we move the tokens at A_{2i-1} and A_{2i} to M_i, for $1 \le i \le 2^k$. Then, there are two tokens at M_i for all $1 \le i \le 2^k$. If we take one token from each of M_1, M_2, $\ldots$, M_{2^k}, then by the induction hypothesis, we can move all of them to the same point, say G. We can do the same with the remaining tokens at M_1, M_2, $\ldots$, M_{2^k}. Thus, all 2^{k+1} tokens are now at G, which completes the induction argument.

   (Here is an alternate approach to the induction step: Given the tokens at A_1, A_2, $\ldots$, $A_{2^{k+1}}$, move the first 2^k tokens to one point G_1, and move the remaining 2^k tokens to one point G_2. Then 2^k more moves can bring all the tokens to the midpoint of G_1 and G_2.)

Presented by the Canadian Mathematical Society and supported by the Actuarial Profession.

Now, assume that n is not a power of 2. Take any line in the plane, and number it as a real number line. (Henceforth, when we refer to a token at a real number, we mean with respect to this real number line.)

At the start, place $n-1$ tokens at 0 and one token at 1. We observed that if we can move all the tokens to the same point, then it must be the centroid of the n points. Here, the centroid is at $\frac{1}{n}$.

We now prove a lemma.

Lemma. *The average of any two dyadic rationals is also a dyadic rational.* (A *dyadic rational* is a rational number that can be expressed in the form $\frac{m}{2^a}$, where m is an integer and a is a nonnegative integer.)

Proof. Consider two dyadic rationals $\frac{m_1}{2^{a_1}}$ and $\frac{m_2}{2^{a_2}}$. Then their average is

$$\frac{1}{2}\left(\frac{m_1}{2^{a_1}}+\frac{m_2}{2^{a_2}}\right) = \frac{1}{2}\left(\frac{2^{a_2}\cdot m_1+2^{a_1}\cdot m_2}{2^{a_1}\cdot 2^{a_2}}\right) = \frac{2^{a_2}\cdot m_1+2^{a_1}\cdot m_2}{2^{a_1+a_2+1}},$$

which is another dyadic rational. ■

On this real number line, a move corresponds to taking a token at x and a token at y and moving both of them to $\frac{x+y}{2}$, the average of x and y. At the start, every token is at a dyadic rational (namely 0 or 1), which means that after any number of moves, every token must still be at a dyadic rational.

But n is not a power of 2, so $\frac{1}{n}$ is not a dyadic rational. (Indeed, if we could express $\frac{1}{n}$ in dyadic form $\frac{m}{2^a}$, then we would have $2^a = mn$, which is impossible unless m and n are powers of 2.) This means that it is not possible for any token to end up at $\frac{1}{n}$, let alone all n tokens.

We conclude that we can always move all n tokens to the same point if and only if n is a power of 2.

2. Let five points on a circle be labelled A, B, C, D, and E in clockwise order. Assume $AE = DE$ and let P be the intersection of AC and BD. Let Q be the point on the line through A and B such that A is between B and Q and $AQ = DP$. Similarly, let R be the point on the line through C and D such that D is between C and R and $DR = AP$. Prove that PE is perpendicular to QR.

   Solution. We are given $AQ = DP$ and $AP = DR$. Additionally $\angle QAP = 180^\circ - \angle BAC = 180^\circ - \angle BDC = \angle RDP$, and so triangles AQP and DPR are congruent. Therefore $PQ = PR$. It follows that P is on the perpendicular bisector of QR.

   We are also given $AP = DR$ and $AE = DE$. Additionally $\angle PAE = \angle CAE = 180^\circ - \angle CDE = \angle RDE$, and so triangles PAE and RDE are congruent. Therefore $PE = RE$, and similarly $PE = QE$. It follows that E is on the perpendicular bisector of PQ.

   Since both P and E are on the perpendicular bisector of QR, the result follows.

3. Two positive integers a and b are *prime-related* if $a = pb$ or $b = pa$ for some prime p. Find all positive integers n, such that n has at least three divisors, and all the divisors can be arranged without repetition in a circle so that any two adjacent divisors are prime-related.

   Note that 1 and n are included as divisors.

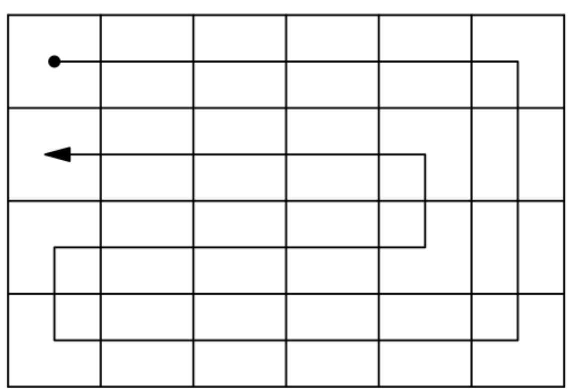
   Solution. We say that a positive integer is *good* if it has the given property. Let n be a good number, and let $d_1, d_2, \ldots, d_k$ be the divisors of n in the circle, in that order. Then for all $1 \le i \le k$, d_{i+1}/d_i (taking the indices modulo k) is equal to either p_i or $1/p_i$ for some prime p_i. In other words, $d_{i+1}/d_i = p_i^{\epsilon_i}$, where $\epsilon_i \in \{1, -1\}$. Then

$$p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k} = \frac{d_2}{d_1} \cdot \frac{d_3}{d_2} \cdots \frac{d_1}{d_k} = 1.$$

   For the product $p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k}$ to equal 1, any prime factor p must be paired with a factor of $1/p$, and vice versa, so k (the number of divisors of n) must be even. Hence, n cannot be a perfect square.

   Furthermore, n cannot be the power of a prime (including a prime itself), because 1 always is a divisor of n, and if n is a power of a prime, then the only divisor that can go next to 1 is the prime itself.

   Now, let $n = p^a q^b$, where p and q are distinct primes, and a is odd. We write the divisors of n in a grid as follows: In the first row, write the numbers $1, q, q^2, \ldots, q^b$. In the next row, write the numbers $p, pq, pq^2, \ldots, pq^b$, and so on. The number of rows in the grid, $a + 1$, is even. Note that if two squares are adjacent vertically or horizontally, then their corresponding numbers are prime-related. We start with the square with a 1 in the upper-left corner. We then move right along the first row, move down along the last column, move left along the last row, then zig-zag row by row, passing through every square, until we land on the square with a p. The following diagram gives the path for $a = 3$ and $b = 5$:



   Thus, we can write the divisors encountered on this path in a circle, so $n = p^a q^b$ is good.

   Next, assume that n is a good number. Let $d_1, d_2, \ldots, d_k$ be the divisors of n in the circle, in that order. Let p be a prime that does not divide n. We claim that $n \cdot p^e$ is also a good number. We arrange the divisors of $n \cdot p^e$ that are not divisors of n in a grid as follows:

$$\begin{array}{cccc} d_1p & d_1p^2 & \cdots & d_1p^e \\ d_2p & d_2p^2 & \cdots & d_2p^e \\ \vdots & \vdots & \ddots & \vdots \\ d_kp & d_kp^2 & \cdots & d_kp^e \end{array}$$

Note that if two squares are adjacent vertically or horizontally, then their corresponding numbers are prime-related. Also, k (the number of rows) is the number of factors of n, which must be even (since n is good). Hence, we can use the same path described above, which starts at d_1p and ends at d_2p. Since d_1 and d_2 are adjacent divisors in the circle for n, we can insert all the divisors in the grid above between d_1 and d_2, to obtain a circle for $n \cdot p^e$.

Finally, let n be a positive integer that is neither a perfect square nor a power of a prime. Let the prime factorization of n be

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}.$$

Since n is not the power of a prime, $t \geq 2$. Also, since n is not a perfect square, at least one exponent e_i is odd. Without loss of generality, assume that e_1 is odd. Then from our work above, $p_1^{e_1} p_2^{e_2}$ is good, so $p_1^{e_1} p_2^{e_2} p_3^{e_3}$ is good, and so on, until $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ is good.

Therefore, a positive integer n has the given property if and only if it is neither a perfect square nor a power of a prime.

4. Find all polynomials $p(x)$ with real coefficients that have the following property: There exists a polynomial $q(x)$ with real coefficients such that

$$p(1) + p(2) + p(3) + \cdots + p(n) = p(n)q(n)$$

for all positive integers n.

Solution. The property clearly holds whenever $p(x)$ is a constant polynomial, since we can take $q(x) = x$. Assume henceforth that $p(x)$ is nonconstant and has the stated property. Let d be the degree of $p(x)$, so $p(x)$ is of the form

$$p(x) = cx^d + \cdots .$$

By a Lemma (which we will prove at the end), $\sum_{k=1}^{n} k^d$ is a polynomial in n of degree $d+1$, so $p(1) + p(2) + \cdots + p(n)$ is a polynomial in n of degree $d+1$. Hence, $q(n)$ is a polynomial of degree 1. Furthermore, the coefficient of n^{d+1} in $\sum_{k=1}^{n} k^d$ is $\frac{1}{d+1}$, so the coefficient of n in $q(n)$ is also $\frac{1}{d+1}$. Let $q(x) = \frac{1}{d+1}(x + r)$. We have that

$$p(1) + p(2) + p(3) + \cdots + p(n) = p(n)q(n)$$

and

$$p(1) + p(2) + p(3) + \cdots + p(n) + p(n+1) = p(n+1)q(n+1).$$

Subtracting the first equation from the second, we get

$$p(n+1) = p(n+1)q(n+1) - p(n)q(n),$$

and hence

$$p(n)q(n) = p(n+1)[q(n+1) - 1].$$

Since this holds for all positive integers n, it follows that

$$p(x)q(x) = p(x+1)[q(x+1) - 1]$$

for all real numbers x. We can then write

$$p(x) \cdot \frac{1}{d+1}(x+r) = p(x+1)\left[\frac{1}{d+1}(x+r+1) - 1\right],$$

so

$$(x+r)p(x) = (x+r-d)p(x+1). \qquad (*)$$

Setting $x = -r$, we get

$$(-d)p(-r+1) = 0.$$

Hence, $-r+1$ is a root of $p(x)$. Let $p(x) = (x+r-1)p_1(x)$. Then

$$(x+r)(x+r-1)p_1(x) = (x+r-d)(x+r)p_1(x+1),$$

so

$$(x+r-1)p_1(x) = (x+r-d)p_1(x+1).$$

If $d = 1$, then $p_1(x)$ is a constant, so both sides are equal, and we can say $p(x) = c(x + r - 1)$.

Otherwise, setting $x = -r + 1$, we get

$$(1 - d)p_1(-r + 2) = 0.$$

Hence, $-r + 2$ is a root of $p_1(x)$. Let $p_1(x) = (x + r - 2)p_2(x)$. Then

$$(x - r - 1)(x + r - 2)p_2(x) = (x + r - d)(x + r - 1)p_2(x + 1),$$

so

$$(x + r - 2)p_2(x) = (x + r - d)p_2(x + 1).$$

If $d = 2$, then $p_2(x)$ is a constant, so both sides are equal, and we can say
$p(x) = c(x + r - 1)(x + r - 2)$.

Otherwise, we can continue to substitute, giving us

$$p(x) = c(x + r - 1)(x + r - 2) \cdots (x + r - d).$$

Conversely, if $p(x)$ is of this form, then

$$\begin{aligned}
p(x) &= c(x + r - 1)(x + r - 2) \cdots (x + r - d) \\
&= \frac{c(d + 1)(x + r - 1)(x + r - 2) \cdots (x + r - d)}{d + 1} \\
&= \frac{c[(x + r) - (x + r - d - 1)](x + r - 1)(x + r - 2) \cdots (x + r - d)}{d + 1} \\
&= \frac{c(x + r)(x + r - 1)(x + r - 2) \cdots (x + r - d)}{d + 1} \\
&\quad - \frac{c(x + r - 1)(x + r - 2) \cdots (x + r - d)(x + r - d - 1)}{d + 1}.
\end{aligned}$$

Then the sum $p(1) + p(2) + p(3) + \cdots + p(n)$ telescopes, and we are left with

$$\begin{aligned}
p(1) + p(2) + p(3) + \cdots + p(n) = &\frac{c(n + r)(n + r - 1)(n + r - 2) \cdots (n + r - d)}{d + 1} \\
&- \frac{c(r)(r - 1) \cdots (r - d + 1)(r - d)}{d + 1}.
\end{aligned}$$

We want this to be of the form

$$p(n)q(n) = c(n + r - 1)(n + r - 2) \cdots (n + r - d)q(n)$$

for some polynomial $q(n)$. The only way that this can hold for each positive integer n is if the term

$$\frac{c(r)(r - 1) \cdots (r - d + 1)(r - d)}{d + 1}$$

is equal to 0. This means r has to be one of the values 0, 1, 2, …, d. Therefore, the polynomials we seek are of the form

$$p(x) = c(x + r - 1)(x + r - 2) \cdots (x + r - d),$$

where $r \in \{0, 1, 2, \ldots, d\}$.

Lemma. *For a positive integer d,*

$$\sum_{k=1}^{n} k^d$$

is a polynomial in n of degree $d+1$. Furthermore, the coefficient of n^{d+1} is $\frac{1}{d+1}$.

Proof. We prove the result by strong induction. For $d = 1$,

$$\sum_{k=1}^{n} k = \frac{1}{2}n^2 + \frac{1}{2}n,$$

so the result holds. Assume that the result holds for $d = 1, 2, 3, \ldots, m$, for some positive integer m. By the Binomial Theorem,

$$(k+1)^{m+2} - k^{m+2} = (m+2)k^{m+1} + c_m k^m + c_{m-1}k^{m-1} + \cdots + c_1 k + c_0,$$

for some coefficients c_m, c_{m-1}, $\ldots$, c_1, c_0. Summing over $1 \le k \le n$, we get

$$(n+1)^{m+2} - 1 = (m+2)\sum_{k=1}^{n} k^{m+1} + c_m \sum_{k=1}^{n} k^m + \cdots + c_1 \sum_{k=1}^{n} k + c_0 n.$$

Then

$$\sum_{k=1}^{n} k^{m+1} = \frac{(n+1)^{m+2} - c_m \sum_{k=1}^{n} k^m - \cdots - c_1 \sum_{k=1}^{n} k - c_0 n - 1}{m+2}.$$

By the induction hypothesis, the sums $\sum_{k=1}^{n} k^m$, $\ldots$, $\sum_{k=1}^{n} k$ are all polynomials in n of degree less than $m+2$. Hence, the above expression is a polynomial in n of degree $m+2$, and the coefficient of n^{m+2} is $\frac{1}{m+2}$. Thus, the result holds for $d = m+1$, which completes the induction step. ■

5. Let k be a given even positive integer. Sarah first picks a positive integer N greater than 1 and proceeds to alter it as follows: every minute, she chooses a prime divisor p of the current value of N, and multiplies the current N by $p^k - p^{-1}$ to produce the next value of N. Prove that there are infinitely many even positive integers k such that, no matter what choices Sarah makes, her number N will at some point be divisible by 2018.

   Solution: Note that 1009 is prime. We will show that if $k = 1009^m - 1$ for some positive integer m, then Sarah's number must at some point be divisible by 2018. Let P be the largest divisor of N not divisible by a prime congruent to 1 modulo 1009. Assume for contradiction that N is never divisible by 2018. We will show that P decreases each minute. Suppose that in the t^{th} minute, Sarah chooses the prime divisor p of N. First note that N is replaced with $\frac{p^{k+1}-1}{p} \cdot N$ where

$$p^{k+1} - 1 = p^{1009^m} - 1 = (p-1)\left(p^{1009^m-1} + p^{1009^m-2} + \cdots + 1\right)$$

   Suppose that q is a prime number dividing the second factor. Since q divides $p^{1009^m} - 1$, it follows that $q \neq p$ and the order of p modulo q must divide 1009^m and hence is either divisible by 1009 or is equal to 1. If it is equal to 1 then $p \equiv 1 \pmod q$, which implies that

$$0 \equiv p^{1009^m-1} + p^{1009^m-2} + \cdots + 1 \equiv 1009^m \pmod q$$

   and thus $q = 1009$. However, if $q = 1009$ then $p \geq 1010$ and p must be odd. Since $p - 1$ now divides N, it follows that N is divisible by 2018 in the $(t+1)^{\text{th}}$ minute, which is a contradiction. Therefore the order of p modulo q is divisible by 1009 and hence 1009 divides $q - 1$. Therefore all of the prime divisors of the second factor are congruent to 1 modulo 1009. This implies that P is replaced by a divisor of $\frac{p-1}{p} \cdot P$ in the $(t+1)^{\text{th}}$ minute and therefore decreases. Since $P \geq 1$ must always hold, P cannot decrease forever. Therefore N must at some point be divisible by 2018.

   Remark (no credit). If k is allowed to be odd, then choosing $k+1$ to be divisible by $\phi(1009) = 1008$ guarantees that Sarah's number will be divisible by 2018 the first time it is even, which is after either the first or second minute.

