Oxford Mathematics Team Challenge 2026

Lock-in Round Solutions

1. Birational correspondences

In this question, we will form two *birational correspondences*. A birational correspondence is a one-one correspondence between two sets such that rational elements of one set pair up with rational elements of the other set. We first consider the unit circle $\mathcal{C}$ given by the equation $x^2 + y^2 = 1$, which is depicted in Figure 1:

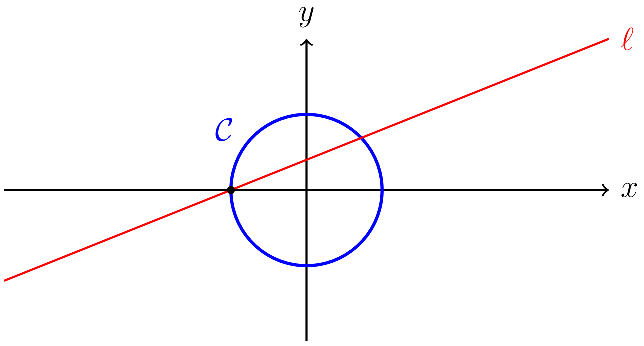


Figure 1

(a) Let ℓ_t be a line with gradient t, where t is some number. We say ℓ_t is a *linking line* if it intercepts $\mathcal{C}$ at $(-1, 0)$.

(i) Any linking line ℓ_t intercepts $\mathcal{C}$ at a second point P_t. Determine the coordinates of P_t in terms of t.

SOLUTION

ℓ_t has gradient t, so its equation is of the form $y = tx + c$; as it passes $(-1, 0)$, $0 = -t + c$ so $c = t$, so ℓ_t is given by $y = t(x + 1)$. To find its intersection we should substitute this into the equation $x^2 + y^2 = 1$:

$$\begin{aligned} x^2 + (t(x+1))^2 &= 1 \\ \implies x^2 - 1 + t^2(x+1)^2 &= 0 \end{aligned}$$

It's actually nicer to not expand here, because we can factorise out $(x + 1)$, which we should be able to do because $x = -1$ is a solution!

$$\begin{aligned} \implies (x+1)\big((x-1) + t^2(x+1)\big) &= 0 \\ \implies (x+1)\big((t^2+1)x + (t^2-1)\big) &= 0 \end{aligned}$$

thus the x-coordinate of P_t is when the second bracket equals zero, i.e. when

$$x = \frac{1 - t^2}{1 + t^2}$$

We can now plug x into ℓ_t to find its y-coordinate:

$$y = t\left(\frac{(1-t^2)}{1+t^2} + \frac{1+t^2}{1+t^2}\right) = \frac{2t}{1+t^2}$$

so the coordinate P_t is given by

$$P_t = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

(ii) Verify that the point P_t found in (a)(i) indeed lies on the circle.

SOLUTION

Indeed,

$$\begin{aligned}\left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 &= \frac{1-2t^2+t^4}{(1+t^2)^2} + \frac{4t^2}{(1+t^2)^2} \\ &= \frac{1+2t^2+t^4}{(1+t^2)^2} \\ &= \frac{(1+t^2)^2}{(1+t^2)^2} = 1\end{aligned}$$

(iii) Write down the equation of the line passing $(-1,0)$ which intercepts with $\mathcal{C}$ at only one point.

SOLUTION

This line must be tangential to $\mathcal{C}$ at $(-1,0)$, so it must be the vertical line $x = -1$.

(b) (i) Let $\mathcal{C}'$ be the points of $\mathcal{C}$ except for $(-1,0)$. Let $P = (a,b)$ be any point in $\mathcal{C}'$. Find the equation of the linking line ℓ_t which intercepts P.

SOLUTION

Given (a,b), we can find the value of t by calculating the gradient between (a,b) and $(-1,0)$:

$$t = \frac{b-0}{a--1} = \frac{b}{a+1}$$

so ℓ_t has the equation $y = \dfrac{b}{a+1}(x+1)$.

(ii) Using parts (a)(i) and (b)(i), briefly deduce that the points in $\mathcal{C}'$ pair up naturally with linking lines – that is, they *correspond* to one another.

SOLUTION

Between any two points lies exactly one line, so the line we found in (b)(i) is unique. And given a linking line ℓ_t, by (a)(i) we can find the point P_t in $\mathcal{C}'$ which ℓ_t intersects.

In particular, these processes are *inverse to each other*: given a linking line ℓ_t, we get a point P_t; the linking line that passes P_t *is* ℓ_t. Conversely, given a point (a, b) we get the line $\ell_{b/(a+1)}$, which then intersects at $P_{b/(a+1)} = (a, b)$. Thus every line will pair up with every point in $\mathcal{C}'$.

INVESTIGATION

In fact, we can use this pairing to find an even more natural pairing between points in $\mathcal{C}$ and *any* line which passes through $(-1, 0)$. Can you see how?

We now show that this correspondence is in fact a *birational correspondence*, in the sense that the line has a rational gradient if, and only if, the point in $\mathcal{C}'$ is "rational" in the following sense:

(c) (i) Let the linking line ℓ_t correspond to the point $P_t = (a, b)$. Show that t is rational if, and only if, a and b are both rational.

SOLUTION

Let $t = p/q$ for integers (whole numbers) p, q with $q \neq 0$. Then by simplifying (a)(i), we get

$$P_t = \left(\frac{q^2 - p^2}{p^2 + q^2}, \frac{2pq}{p^2 + q^2} \right)$$

so a and b are both rational, as they're both ratios of integers; also note they're well-defined, as $p^2 + q^2 \geq 0$ (sum of squares is non-negative) but as $q \neq 0$ in fact $p^2 + q^2 \neq 0$.

On the other hand, suppose $a = p/q$ and $b = r/s$ for integers p, q, r, s with $q, s \neq 0$. Then by simplifying (b)(i), we get

$$t = \frac{rq}{(p + q)s}$$

which is also the ratio of integers. We know $s \neq 0$, but is $p + q \neq 0$? If $p + q = 0$, then $p = -q$ so $a = -1$, but then this would be the point $(-1, 0)$ which isn't paired up with a linking line.

(ii) Hence, write down the general form for points (a, b) in $\mathcal{C}'$ where a and b are both rational. *[Your general form should be in terms of whole numbers p and q.]*

SOLUTION

So the general form is

$$\left(\frac{q^2 - p^2}{p^2 + q^2}, \frac{2pq}{p^2 + q^2}\right)$$

Note that this *is* the general form: by (c)(i), if (a, b) is a rational point then it corresponds to a linking line ℓ_t, with t rational. As t is rational, $t = p/q$ for some p, q with $q \neq 0$ which recovers the equation given above.

(d) (i) A *Pythagorean triple* is a triple of positive whole numbers (a, b, c) such that $a^2 + b^2 = c^2$.

Using previous parts, or otherwise, find a general form for a Pythagorean triple in terms of two positive whole numbers p, q with $q > p > 0$. *[The general form $(a, b, \sqrt{a^2 + b^2})$ is* not *general because $\sqrt{a^2 + b^2}$ is not necessarily whole.]*

SOLUTION

Take the general solution from (c)(ii) and plug it into the equation for $\mathcal{C}$:

$$\left(\frac{q^2 - p^2}{p^2 + q^2}\right)^2 + \left(\frac{2pq}{p^2 + q^2}\right)^2 = 1$$

By multiplying up by $(p^2 + q^2)^2$, we get

$$(q^2 - p^2)^2 + (2pq)^2 = (p^2 + q^2)^2$$

which satisfies the equation of a Pythagorean triple.

(ii) Suppose (a, b, c) is a Pythagorean triple where a, b, c have highest common factor 1. Carefully explain why (a, b, c) *or* (b, a, c) is part of the general form you found in (d)(i).

SOLUTION

As $a^2 + b^2 = c^2$, $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$ (note $c \neq 0$). This is a rational point in $\mathcal{C}'$ (it won't be $(-1, 0)$ as $b \neq 0$) so it corresponds to a rational value of t which generates p, q such that

$$\frac{a}{c} = \frac{q^2 - p^2}{p^2 + q^2} \quad \text{and} \quad \frac{b}{c} = \frac{2pq}{p^2 + q^2}$$

multiplying up, we get that (a, b, c) is part of our general form. We might need to switch a and b around if, for example, b is odd.

(iii) If (a, b, c) is a Pythagorean triple where a, b, c have highest common factor $h > 1$, will they be part of the general form you found in (d)(i)? *[Hint: consider $a = 9$.]*

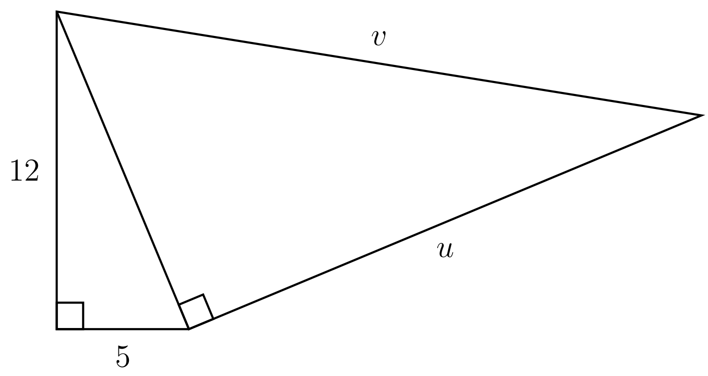
SOLUTION

No! As hinted, consider $a = 9$ which leads us to consider the Pythagorean triple $(9, 12, 15)$. As a is odd and b isn't, we'll need $9 = q^2 - p^2$ and $12 = 2pq$, so $15 = q^2 + p^2$. But then, for example, $2q^2 = 24$ which would mean q is not whole – a contradiction.

INVESTIGATION

Can you think of a "quick fix" so that we can get a general formula for any Pythagorean triple?

(iv) Hence, find the unique positive whole numbers u, v which satisfy the following diagram (which is very much *not* to scale):



SOLUTION

The hypotenuse of the triangle with side-lengths 5 and 12 is 13. So we want to find u and v such that $13^2 + u^2 = v^2$; we can use the form from (d)(i) to find it. We spot $13 = 7^2 - 6^2$ as $7^2 - 6^2 = (7-6)(7+6)$, so $u = 2 \times 6 \times 7 = 84$ and $v = 6^2 + 7^2 = 85$.

Alternatively, as $13^2 + u^2 = v^2$, $13^2 = (v - u)(v + u)$. We only have a few combinations to try: $v - u = 13$ and $v + u = 13$ gives $u = 0$ (no good), but $v - u = 1$ and $v + u = 169$ gives the correct values.

INVESTIGATION

What if we replace 5 and 12 with **(a)** 3 and 4; **(b)** 8 and 15; **(c)** 7 and 24?

Now let $\mathcal{E}$ be the ellipse given by $x^2 + y^2 - xy = 1$, as depicted in Figure 2:

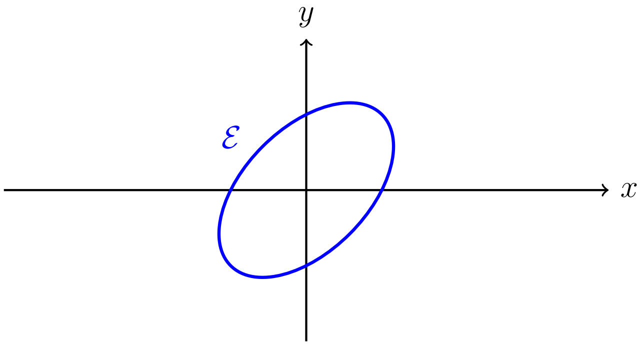


Figure 2

(e) By considering lines that intercept $(1, 0)$, or otherwise, find all pairs of rational numbers (x, y) which satisfy $x^2 + y^2 - xy = 1$ (in terms of whole numbers p and q).

SOLUTION

We essentially do the same strategy to find rational points as in (a)(i). A general line passing $(1, 0)$ is of the form $y = t(x-1)$, except for the line $x = 1$ (don't forget about this line!). Call these *linking lines* as before; we should plug the equation of a linking line into the ellipse equation:

$$x^2 + t^2(x-1)^2 - xt(x-1) = 1$$

Again, it's nicer to not expand and to factorise $(x - 1)$, which again we should expect (we've set this equation up *so that* it passes through $(1, 0)$!):

$$\begin{aligned}
\implies (x^2 - 1) + t^2(x-1)^2 - tx(x-1) &= 0 \\
\implies (x-1)\big((x+1) + t^2(x-1) - tx\big) &= 0 \\
\implies (x-1)\big(x(t^2 - t + 1) + (1 - t^2)\big) &= 0
\end{aligned}$$

so the other point of intersection has x-coordinate

$$x = \frac{t^2 - 1}{t^2 - t + 1}$$

Note the denominator is never zero, because the discriminant of t^2+t+1 is $-3 < 0$. Plugging this into the linking line ℓ_t, we get the y-value

$$y = t\left(\frac{t^2 - 1}{t^2 - t + 1} - \frac{t^2 - t + 1}{t^2 - t + 1}\right) = \frac{t^2 - 2t}{t^2 - t + 1}$$

By setting $t = p/q$, we can then find the rational parametrisation of $\mathcal{E}$:

$$\left(\frac{p^2-q^2}{p^2-pq+q^2}, \frac{p^2-2pq}{p^2-pq+q^2}\right), \qquad p, q \in \mathbb{Z},\ q \neq 0$$

We need to remember the line $x = 1$...! This line intersects the points $(1, 1)$, which our parametrisation misses, although conveniently enough if we allow $p = 1$ and $q = 0$ we recover it on our rational parametrisation; so in fact a general rational solution is

$$\left(\frac{p^2-q^2}{p^2-pq+q^2}, \frac{p^2-2pq}{p^2-pq+q^2}\right), \qquad p, q \in \mathbb{Z},\ p, q \text{ not both } 0.$$

INVESTIGATION

In fact, changing to 'p, q not both 0' is a little bit more than "convenient" – there are no coincidences in mathematics! This question – or generally the existence of *birational correspondences* – has to do with a branch of mathematics called *projective geometry*, which has many characterisations, although one way to characterise it is as formalising *perspective art* where you add lines or points "at infinity".

I first came across projective geometry with this video, by Bill Shillito, which I highly recommend:

https://www.youtube.com/watch?v=XXzhqStLG-4

Learning about projective geometry more properly/formally is quite hard, because linear algebra (roughly speaking, deeper theory about matrices and vectors) is essentially a prerequisite, but it's definitely interesting to learn a bit about, and I think the video above gives a nice introduction to it with the visual appeal that projective geometry deserves.

One way to motivate projective geometry is this: the quadratic equation

$$ax^2 + bx + c = 0$$

sometimes has two real solutions, however when we add complex numbers and count repeated roots, it *always* has two. One might hope the same idea goes for a quadratic curve intersecting a line – there can *sometimes* be two intersections, or perhaps one tangentially, however projective geometry is the analogue to complex numbers in that it helps to guarantee that there are always two intersections (this follows from what is called *Bézout's Theorem*).

How many times does $y = x^2$ intersect $y = 2x+3$, $y = 0$, $y = x-3$, $x = 0$? Between counting multiplicity of roots, adding complex numbers, and projectivising the plane, which are needed to "find" two solutions for each of these lines?

2. Look-and-say sequences

In this question, we will discuss *look-and-say sequences*, invented by John Conway. Define a *good number* to mean a positive integer that does not contain ten or more equal digits in a row. A look-and-say sequence is an infinite sequence $L_1, L_2, L_3, \ldots$, where the first term L_1 is a good number, and each term afterwards is defined by this recursive rule:

1. Partition the digits of the current term into non-overlapping groups of consecutive digits, where each group consists of equal digits, and neighbouring groups have different digits. We will refer to these groups as *runs*.

2. From left to right, for each run, say the number of digits in that run, followed by the digit of that run. The numbers you say are the digits of the next term.

For example, if $L_1 = 113$, then the runs are 11 and 3, so you read out 113 as "two 1s, one 3", giving you $L_2 = 2113$. Then the runs of 2113 are 2, 11, and 3, so you read out 2113 as "one 2, two 1s, one 3", giving you $L_3 = 122113$, and so on.

Throughout this problem, you should disregard cases where a term has a run of ten or more digits, such as 1111111111. You may assume without proof that if L_1 is a good number, then all terms L_n are good numbers.

(a) Consider the look-and-say sequence with $L_1 = 1$.

(i) Compute L_7 and L_8. No justification needed.

SOLUTION

We get $L_7 = 13112221$ and $L_8 = 1113213211$.

(ii) Find the last two digits of L_{2026}. No justification needed.

SOLUTION

Starting from L_2, the last two digits of each term alternate between 11 and 21. In particular, the last two digits of L_n is 11 whenever n is even, therefore the last two digits of L_{2026} is 11.

(b) (i) Call a digit in a number *switched* if it is a non-leading digit that is not equal to the digit immediately before it. Given that L_n has d switched digits, write an expression in terms of d for the number of digits in L_{n+1}. No justification needed.

SOLUTION

Any run of L_n begins with either the leading digit of L_n or with a switched digit, so L_1 has $1 + d$ runs. We say two numbers for each run, so the number of digits in L_{n+1} is double the number of runs in L_n. The number of digits in L_{n+1} is $2(1 + d) = 2 + 2d$.

(ii) Briefly explain why all the terms in a look-and-say sequence share the same last digit.

SOLUTION

Say the last digit of L_n is x. The last run of L_n consists of xs, which you would read as "[some number] xs", meaning the last digit of L_{n+1} is also x. Since neighbouring terms in the sequence share the same last digit, then all terms do.

(c) A good number x is called a *fixed point* if setting $L_1 = x$ results in a sequence where all L_n are equal. In this part, you will work towards proving that there only is one fixed point, namely 22.

(i) Using the definition, show that 22 is a fixed point. Explain carefully.

SOLUTION

If $L_n = 22$, then we would read it as "two 2s", meaning $L_{n+1} = 22$. By the definition of fixed point, 22 is a fixed point because setting $L_1 = 22$ means $L_2 = L_1 = 22$, and $L_3 = L_2 = 22$, and so on because $L_{n+1} = L_n = 22$ for all $n \geq 1$.

(ii) Suppose x is a fixed point with leading digit d. Explain briefly why the first run of x contains d digits.

SOLUTION

Note that the leading digit of L_2 says how many digits are in the first run of L_1. If L_1 is a fixed point with leading digit d, then L_2 also has leading digit d since $L_1 = L_2$, meaning that L_1 begins with a run of d occurrences of the digit d.

(iii) By referencing the statement in (c)(ii), or otherwise, show that any fixed point must have a leading digit of 2.

SOLUTION

Let L_1 be a fixed point. Using a proof by contradiction, we can show that any fixed point cannot have a leading digit other than 2.

Suppose the leading digit of L_1 is 1. First, L_1 must have more than one digit because 1 is not a fixed point. By (c)(ii), the first digits of L_1 are $1a\ldots$ for some $a \neq 1$. But then $L_2 = 11ba\ldots$, so L_2 differs from L_1 at the second digit. This is a contradiction, so the leading digit of L_1 cannot be 1.

Suppose that the leading digit of L_1 is 3. By (c)(ii), L_1 begins with $333\ldots$. Then the second run of L_1 must be three digits long also, since the third digit of L_2 is 3. This means that L_1 begins $333aaa\ldots$. But L_2 would be describing L_1 as "three 3s, three as, a as, …", and this is impossible since we do not allow the second and third run to consist of the same digit. This is a contradiction, so the leading digit of L_1 cannot be 3.

Suppose that the leading digit of L_1 is 4 or greater. Then by (c)(ii), L_1 begins with at least four equal digits, so $L_2 = L_1 = aaaa\ldots$, which is impossible because we would have the first and second runs consisting of the same digit. This is a contradiction, so the leading digit of L_1 cannot be 4 or greater. Therefore, any fixed point must have a leading digit of 2.

(iv) By referencing the statements in the previous subparts, or otherwise, show that 22 is the only fixed point.

SOLUTION

By (c)(i), 22 is a fixed point. Suppose that y is a fixed point not equal to 22. By (c)(iii), y must have leading digit of 2. By (c)(ii), y begins with the digits $22\ldots$, and there exist $k \geq 1$ digits $a_1, \ldots, a_k$ such that $y = 22a_1\ldots a_k$. Notice that $a_1 \neq 2$ because the first run of y is two digits long, and that y can only be a fixed point if $a_1 \ldots a_k$ is one as well. This is impossible by (c)(iii) since $a_1 \neq 2$, so by contradiction, y cannot exist. Therefore, 22 is the only fixed point.

(d) Returning to the look-and-say sequence with $L_1 = 1$, let D_n be the number of digits in L_n. It turns out that the sequence $D_1, D_2, D_3, \ldots$ grows approximately exponentially, with the ratio D_{n+1}/D_n approaching λ as n grows; λ is known as *Conway's constant.* We will approximate Conway's constant using probability.

(i) Explain why the only digits that appear in the look-and-say sequence with $L_1 = 1$ are 1, 2, and 3.

SOLUTION

Consider the digits in even positions of L_n (i.e. second digit, fourth digit, etc.). Digits in neighbouring even positions must be different, because the even digits describe the digits in the runs of L_{n-1}, and neighbouring runs must contain different digits. Thus, the largest number of equal consecutive digits we can have is 3, so the largest digit we can have is 3. Note that 0 cannot appear because L_1 does not contain 0, and there is no way to introduce a 0 later on as there will not be any runs of length 0.

(ii) Let n be a large positive integer. In order to make your approximation, you should make the following simplifying assumption. Since L_n only consists of 1, 2, and 3, assume that the digits in L_n are sampled independently at random with a 1/3 probability of each of 1, 2, and 3.

Let r be an approximation of the growth rate D_{n+1}/D_n. Give a value for r, and show how you arrived at this value. Your approximation need not match the official answer if you justify your answer quantitatively.

SOLUTION

Recall from (b)(i) that if L_n has d switched digits, then $D_{n+1} = 2 + 2d$. A non-leading digit of L_n is a switched digit when it is unequal to the digit immediately before it. Using the simplifying assumption, the probability of that happening is 2/3 for each non-leading digit. There are $D_n - 1$ non-leading digits of L_n, so the number of switched digits is about $\frac{2}{3}(D_n - 1)$. Then we estimate $D_{n+1} = 2 + 2(\frac{2}{3}(D_n - 1)) = \frac{4}{3}D_n + \frac{2}{3}$. Then we approximate r by

$$r = \frac{D_{n+1}}{D_n} = \frac{(\frac{4}{3}D_n + \frac{2}{3})}{D_n} = \frac{4}{3} + \frac{2}{3D_n}.$$

Since n is a large integer, then D_n is very large too, so $\frac{2}{3D_n} \approx 0$. This method of approximation gives us $r = \frac{4}{3}$.

(iii) The actual value of Conway's constant is $\lambda \approx 1.3036$. Compare your r from the previous subpart to λ. If $r > \lambda$, explain one way in which the simplifying assumption may have led you to overestimate λ. If $r < \lambda$, explain one way in which the simplifying assumption may have led you to underestimate λ.

SOLUTION

The official answer's approximation is an overestimate of λ. One possible reason for the overestimate is that the simplifying assumption assigns an equal probability to 1, 2, and 3, when in reality there may be one digit that is quite likely and two that are less common. As a result there will be fewer switched digits, hence fewer digits in D_{n+1} (in fact, for large L_n, there are almost twice as many 2s as there are 3s, and almost thrice as many 1s as 3s).

If a competitor's value for r is an underestimate, the best explanation they can give is that the assumption of digits sampled independently allows for runs of longer than three digits, which is not possible in reality. Allowing long runs means allowing long droughts of no switched digits, so the assumption underestimates the number of switched digits and hence underestimates D_{n+1}.

Competitors may propose other possible explanations, but they must be correct and specific to the direction of skew. For example, simply citing the assumption of independence is insufficient for full marks, without explaining why it leads to an overestimate instead of underestimate, or vice versa.

(iv) It turns out for any good number $L_1 \neq 22$, the sequence $D_1, D_2, D_3, \ldots$ grows exponentially at the same rate λ. If a look-and-say sequence with a different L_1 consists only of the digits 1, 2, and 3, then the simplifying assumption still applies, and r will be the same as before.

Explain why even if a look-and-say sequence contains digits other than 1, 2, and 3, you can still justifiably use the simplifying assumption to produce the same r.

SOLUTION

Define a *bad digit* as any digit other than 1, 2, and 3. For any good number L_1, there are no runs in L_2 longer than three digits. As such, the number of bad digits in L_n is bounded above by the number of bad digits in L_2, since there is no way to introduce more bad digits in the sequence. The number of bad digits does not grow, but the total number of digits grows without bound, so as n gets large, the proportion of bad digits to total digits approaches 0. This means that for large L_n, the bad digits have a negligible effect on the proportion of switched digits, so the simplifying assumption still applies.

3. Confused coats

Carol has a collection of six coats labelled A, B, C, D, E, F, and six coat hooks labelled 1, 2, 3, 4, 5, 6. Currently the coats are in *starting order*: coat A is on hook 1, coat B is on hook 2, and so on. The starting order *reads* from left to right as $ABCDEF$.

A *swap* is a pair of distinct numbers written $(m\ n)$ indicating that we should swap the coats on hooks m and n. For example, if we perform $(2\ 5)$ from starting order, then the coats read $AECDBF$ from left to right.

(a) Steve performs the swap $(m\ n)$ on starting order. Write down the swap that Carol should perform to return the coats to starting order.

SOLUTION

The swap $(m\ n)$, or equivalently $(n\ m)$, will undo Steve's swap.

We can perform multiple swaps in a row by performing the left-most swap first. For example, $(1\ 2)(2\ 3)$ denotes performing the swap $(1\ 2)$ first, followed by the swap $(2\ 3)$.

(b) (i) Perform $(1\ 3)(2\ 4)(3\ 5)$ on starting order. What do the coats read from left to right?

SOLUTION

One way to compute these is to pick a number and "follow it along" from left to right. For example, following coat A, it swaps to hook 3, and then hook 3 swaps with hook 5, so $A \mapsto 5$. Doing this, the permutation is overall $(1\ 5\ 3)(2\ 4)$ so the coats will read $CDEBAF$.

INVESTIGATION

Perform the following permutations on starting order. What do the coats read from left to right?

(a) $(1\ 3)(2\ 4)(3\ 5)(4\ 5\ 6)$

(b) $(1\ 3\ 5)(2\ 4\ 6)(3\ 5\ 1)$

(c) $(1\ 2\ 3\ 4\ 5\ 6)(1\ 2\ 3\ 4\ 5)(1\ 2\ 3\ 4)(1\ 2\ 3)(1\ 2)(1)$

(ii) Steve performs the swaps in (b)(i) on starting order. Write down a series of swaps that Carol can perform to return the coats to starting order.

SOLUTION

If we perform the swaps that Steve did *in reverse order*, we will return the coats to starting order, so we should perform $(3\ 5)(2\ 4)(1\ 3)$.

(c) Imagine, for this part only, that Carol in fact has one hundred coats labelled C_1, C_2, ..., C_{100}, and one hundred coat hooks labelled 1, 2, 3, ..., 100. For each of the following series of swaps, write down what the coats read from left to right:

(i) $(1\ 2)(1\ 3)(1\ 4)\dots(1\ 100)$;

SOLUTION

Following coat 1, it gets sent to 2 by the first swap and the remaining 98 swaps don't move coat 2, so $1 \mapsto 2$. If we now consider coat C_2, it gets swapped to hook 1 at the start, which gets swapped to hook 3 in the next swap, so $C_2 \mapsto 3$. Generally, coat C_n will swap with hook 1 on the $(n-1)$th swap, and then will swap with hook $n+1$ on the nth swap, with the exception of coat C_{100} which gets sent to hook 1. So the coats should read

$$C_{100}C_1C_2C_3\dots C_{98}C_{99}$$

(ii) $(1\ 2)(2\ 3)(3\ 4)\dots(99\ 100)$.

SOLUTION

Similarly to (c)(i), following coat C_1 swaps with hook 2, then swaps to hook 3, ..., then to hook 100, so $C_1 \mapsto 100$. For any other coat C_n, it swaps with hook $n-1$ which then doesn't get touched for the rest of the permutation, so $C_n \mapsto n-1$ for $n \neq 1$. So the coats will read

$$C_2C_3C_4\dots C_{99}C_{100}C_1$$

A *cycle* is a series of distinct numbers $(n_1\ n_2\ \dots\ n_k)$, indicating that move each coat to the next position in the cycle, and move the last coat to the first position. For example, performing $(2\ 5\ 4)$ on starting order reads $ADCEBF$ from left to right.

Similarly with swaps, we may perform a series of cycles starting with the left-most cycle first. A series of cycles is called a *permutation*; we say two permutations are *the same* if they produce the same left-to-right reading of coats on the hooks.

(d) (i) Show that any cycle is the same as a series of swaps.

SOLUTION

We can use (c) to algorithmically find a series of swaps. For any cycle $(n_1\ n_2\ n_3\ n_4\ \dots\ n_k)$, the series of swaps

$$(n_1\ n_2)(n_1\ n_3)(n_1\ n_4)\dots(n_1\ n_k)$$

will be the same.

(ii) Hence, deduce that for any permutation σ that Steve applies to the coats, there is some permutation that returns the coats to starting order.

SOLUTION

We should check each coat to see it gets mapped to the same place. Clearly any coat on hook n or hook p get sent to the same hook (hooks p and q respectively); we also see the same holds for m and q.

We call this permutation its *inverse* and denote it by σ^{-1}. You may use, without proof, the fact that it is unique (that is, if σ_1^{-1} and σ_2^{-1} both return the coats to starting order after Steve applies σ, then σ_1^{-1} is the same as σ_2^{-1}).

INVESTIGATION

Can you prove that the inverses of permutations are unique?

(iii) Using (d)(i), or otherwise, find a series of *exactly four* swaps which is the same as the permutation $(2\ 6\ 4\ 5)(2\ 4\ 5)(4\ 1\ 3\ 5)$. *[Hint: it is useful to note that, for example, the cycle $(m\ n\ p\ q)$ is the same as the cycle $(n\ p\ q\ m)$.]*

SOLUTION

We can manipulate these cycles with (d)(i) and the hint, and use the fact that having two of the same swap next to each other "cancel out" (a) to simplify this permutation. So we have

$$\begin{aligned}
&(2\ 6\ 4\ 5)(2\ 4\ 5)(4\ 1\ 3\ 5) && \\
&= (2\ 6\ 4\ 5)(5\ 2\ 4)(5\ 4\ 1\ 3) && \text{by hint} \\
&= (2\ 6)(2\ 4)\underbrace{(2\ 5)(5\ 2)}_{\text{cancels}}\underbrace{(5\ 4)(5\ 4)}_{\text{cancels}}(5\ 1)(5\ 3) && \text{by (d)(i)} \\
&= (2\ 6)(2\ 4)(5\ 1)(5\ 3) && \text{by (a)}
\end{aligned}$$

so we are done.

(iv) How many different permutations are there? Briefly explain.

SOLUTION

By performing any series of cycles, we can reach any reordering of $ABCDEF$, so the question is really how many ways there are to order six distinct coats. The answer to this is $6! = 720$.

Let σ be a permutation and write σ^k to denote applying σ on the coats k times in a row (if $k = 0$, we do nothing). The *order* of σ is the least $k > 0$ such that σ^k is the same as doing nothing, or put differently, applying σ^k on starting order reads $ABCDEF$.

(e) Find the orders of the following permutations:

(i) $\sigma_1 = (2\ 3\ 5)(1\ 4\ 6)$;

SOLUTION

Looking ahead, it is useful to use the fact that these two cycles are disjoint since two cycles being disjoint essentially means they don't "affect one another". After three applications of σ_1 the cycles will cancel themselves out, and clearly one or two applications of σ_1 does not return the coats to starting order. So the order of σ_1 is 3.

(ii) $\sigma_2 = (2\ 3\ 5)(1\ 4)$;

SOLUTION

Likewise, these two cycles don't affect each other, but as they're of different lengths they don't easily line up in doing nothing at the same time. Every two cycles, $(1\ 4)^2$ does nothing, and every three cycles, $(2\ 3\ 5)^3$ does nothing. So we want the lowest common multiple of these, which is 6; so the order of σ_2 is 6.

(iii) $\sigma_3 = (2\ 3\ 5)(5\ 6)$.

SOLUTION

We should rework σ_3 to be a series of disjoint cycles (looking ahead at the note after (f)(iii), we know that this will work). Indeed, $(2\ 3\ 5)(5\ 6) = (2\ 3\ 6\ 5)$, so the order of σ_3 is 4.

INVESTIGATION

What is the order of a general permutation on Carol's coats?

INVESTIGATION

One thing we assumed in this question was that an order exists at all! In some similar mathematical structures there are elements with *infinite orders*, which is to say there is no $k > 0$ such that σ^k does nothing.

(a) Prove that permutations on Carol's coats do have a (finite) order.

(b) Come up with an example of a structure with infinite-order elements.

We also say two cycles $(a_1\ a_2\ \dots\ a_k)$ and $(b_1\ b_2\ \dots\ b_\ell)$ are *disjoint* if $a_i \neq b_j$ for all i, j.

(f) (i) By following one of the coats, show that

$$(a_1\ a_2\ \dots\ a_k)(b_1\ b_2\ \dots\ b_\ell) \qquad \text{and} \qquad (b_1\ b_2\ \dots\ b_\ell)(a_1\ a_2\ \dots\ a_k)$$

are the same permutation if the two cycles are disjoint.

SOLUTION

Label the coats $C_1, C_2, \dots, C_6$ instead of $A, B, \dots, F$. Following coat C_n, as the two cycles are disjoint either n is equal to one of $a_1, \dots, a_k$ or one of $b_1, \dots, b_\ell$ or neither. If neither, then neither of the cycles affect coat C_n. If $n = a_i$ for some i, then C_n maps to hook a_{i+1}; this doesn't get sent anywhere with the b-cycle as a_{i+1} isn't any of the b_j's (as the cycles are disjoint). By symmetry C_n won't behave badly if n is one of the b_j's; as these two permutations send any coat to the same hook, they must be the same.

(ii) Does the result in (g)(i) hold even if the two permutations are not disjoint? Briefly justify your answer.

SOLUTION

No: $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$ as the left-hand permutation equals the cycle $(1\ 3\ 2)$ and the right-hand permutation equals the cycle $(2\ 3\ 1)$ which aren't the same (they don't send coat B to the same hook, for example).

(iii) Let σ be a permutation. By considering the permutations

$$\sigma^0,\ \sigma^1,\ \sigma^2,\ \sigma^3,\ \dots$$

deduce that there is some $k > 0$ such that σ^k keeps coat A on hook 1.

SOLUTION

Since there are only six hooks, two of the permutations σ^m and σ^n will send coat A to the same hook.

It turns out that, using (f)(iii), one can show that *any* permutation is the same as a series of disjoint cycles. You may use this result in part (g) without proof.

INVESTIGATION

Let's see if we can prove it! With (f)(iii), it follows that we can write σ as a cycle including A and then some other stuff. **(a)** Finish the argument. **(b)** To what extent is the series of disjoint cycles unique?

(g) (i) How many different permutations are there with order 6?

SOLUTION

For a permutation to have order 6, it must break into disjoint cycles of length 2, 3, and 6. If there is no cycle of length 6, there must be at least one cycle of length 2 and one cycle of length 3. Since we only have 6 coats, our two cases are 1 cycle of length 6 or 2 disjoint cycles, one of length 2 and one of length 3.

Case 1: 1 cycle of length 6

We must use precisely all 6 elements, and there are $6! = 720$ ways to order them in our cycle. However, as mentioned in the hint in (d)(iii), as long as the order is preserved, the starting element does not matter, so we must divide by 6 to get 120 cycles of length 6.

Case 2: 2 disjoint cycles, one of length 2 and one of length 3

There are ${}^6C_2 = 15$ ways to choose the coats for the cycle of length 2 and ${}^4C_3 = 4$ ways to choose the coats for the length of length 3 from the remaining coats.

Again, there are $3!/3 = 2$ ways to order the coats to create different cycles of length 3 and $2!/2 = 1$ way to order the coats to create different cycles of length 2. Hence, this case has $15(4)(2) = 120$ permutations.

No permutation can fall in both cases since the permutations in each case fix different number of coats in their original place (0 and 1, respectively).

All together, we have $120 + 120 = 240$ permutations of order 6.

(ii) How many different permutations are there with order 3?

SOLUTION

For a permutation to have order 3, it must break into disjoint cycles of length 3. Since we have 6 coats, our two cases are either 1 or 2 disjoint cycles of length 3.

Case 1: 1 cycle of length 3

There are ${}^6C_3 = 20$ ways to choose the 3 elements for the cycle of length 3 and $3!/3 = 2$ different ways to order them to create different cycles, giving 40 permutations in this case.

Case 2: 2 disjoint cycles of length 3 There are ${}^6C_3 = 20$ ways to choose the 3 elements the first cycle and ${}^3C_3 = 1$ way to choose the elements for the second cycle. However, the order we list these cycles do not matter, so we must divide by 2. For both of these cycles, there are $3!/3 = 2$ different ways to order their coats to create different cycles, giving $20(1)(2)(2)/2 = 40$ permutations in this case.

Note that a permutation cannot break into different sets of cycles of length 3 in different cases because the permutations in each case fix different amounts of coats in their original place (3 and 0, respectively).

All together, we have $40 + 40 = 80$ permutations of order 3.

(iii) How many different permutations are there with order 2?

SOLUTION

For a permutation to have order 2, it must break into a series of disjoint cycles all of order 2. We can then count them based on how many cycles they break into: 1, 2, and 3.

Case 1: 1 cycle of length 2

There are ${}^6C_2 = 15$ ways to choose 2 coats to swap in 1 2-cycle.

Case 2: 2 disjoint cycles of length 2

There ${}^6C_2 = 15$ ways to choose the first 2 coats and then ${}^4C_2 = 6$ ways to choose the second 2 coats to create 2 disjoint cycles of length 2. Additionally, since the order we list the swaps do not matter, we must then divide by 2 to get $15(6)/2 = 45$ permutations of this kind.

Case 3: 3 disjoint cycles of length 2

There are ${}^6C_2 = 15, {}^4C_2 = 6$, and ${}^2C_2 = 1$ ways to choose the coats for the first, second, and third disjoint cycle of length 2, respectively. Again, order does not matter, so divide by $3! = 6$ to get $15(6)(1)/6 = 15$ permutations of this kind.

Note that a permutation cannot break into different sets of cycles of length 2 in different cases because the permutations in each case fix different amounts of coats in their original place (4, 2, and 0, respectively).

All together, we have $15 + 45 + 15 = 75$ permutations of order 2.

INVESTIGATION

What are the possible orders of permutations (of Carol's coats)?