5A Permutations

5A1 (Derangements) In an exercise session there are n students numbered $1, 2, \ldots, n$. Each hands a solution paper to the TA, who permutes them to some order, and hands them back to students for peer grading. Let the tuple $(a_1, a_2, \ldots, a_n)$ indicate the permutation: for each i, student i is grading the paper of student a_i.

There are $n!$ ways how the papers can be permuted. We want to find how many of these ways are *derangements*, meaning that $a_i \neq i$ for all $1 \leq i \leq n$ (nobody is grading their own paper).

(a) For each $n \in \{1, 2, 3, 4\}$, list explicitly all derangements, and count them. Then make a table with four columns: n, D_n (the number of derangements), $n!$, and the ratio $D_n/n!$.

When listing the derangements for $n = 4$, proceed systematically making consecutive choices, and draw a branching diagram: First, list the three choices for a_1; from each of them, draw branches for the possible choices for a_2, then for a_3, and then for a_4. If on some branch you reach impossibility (you cannot make a valid choice), mark that branch a “dead end”, and do not count it.

(b) Study the structure of your $n = 4$ diagram, particularly the numbers of branches on various levels. Does it look regular?

(c) From lectures/notes/slides, find the formula for the exact number of derangements (the one that contains a *finite* summation $\sum_{k=0}^{n}$). Applying that formula, calculate D_n for $1 \leq n \leq 5$. Verify that it matches (a) for $n \leq 4$.

(d) (OPTIONAL, not required, no points) Go to `https://oeis.org` and enter your known five values of D_n. Verify that you found something that talks about derangements.

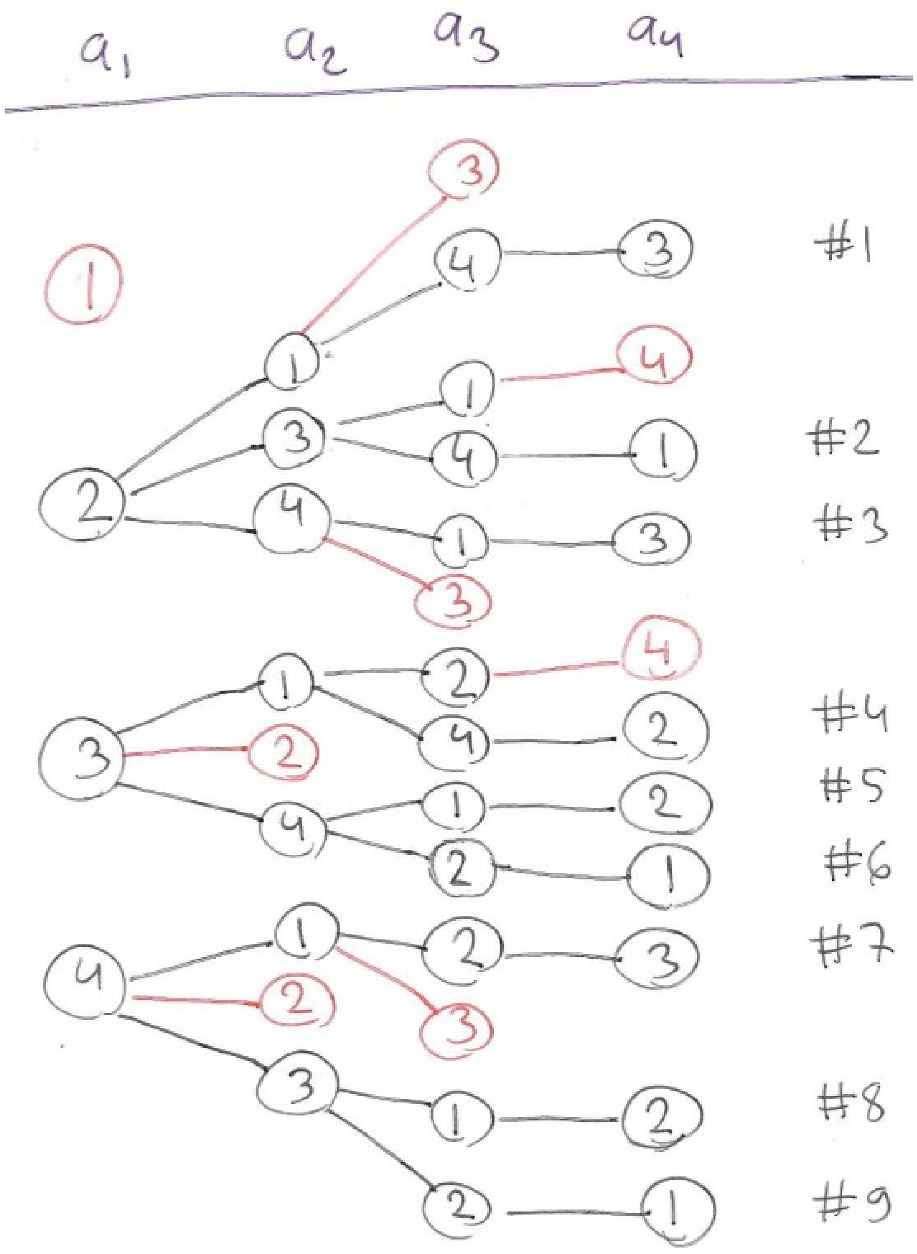
(e) (OPTIONAL, not required, no points) Study what happens to your OEIS findings if you enter fewer values, or miscalculate one of them (e.g. decrease a_5 by one, simulating that you tried to list but missed one case); etc.

Without going deeper into probability theory: If we consider that each of the $n!$ possible arrangements is equally likely to happen, then $D_n/n!$ is the probability for the event that “nobody is grading their own paper”.

Solution.

(a)

n	D_n	$n!$	$D_n/n!$
1	0	1	0
2	1	2	$\frac{1}{2}$
3	2	6	$\frac{1}{3}$
4	9	24	$\frac{3}{8}$



(b) There doesn't seem to be any simple, clear, or intuitive rule that would predict the number of derangements in each branch or which branches get terminated, or at what level they get terminated.

(c)

$$D_n = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}$$

$$\begin{aligned}
D_1 &= 1 \cdot (1-1) = 0 \\
D_2 &= 2 \cdot (1 - 1 + \frac{1}{2}) = 1 \\
D_3 &= 6 \cdot (1 - 1 + \frac{1}{2} - \frac{1}{6}) = 2 \\
D_4 &= 24 \cdot (1 - 1 + \frac{1}{2} - \frac{1}{6} + \frac{1}{24}) = 9 \\
D_5 &= 120 \cdot (1 - 1 + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120}) = 44
\end{aligned}$$

5A2 (Notation and composition) Consider the permutation π whose two-line notation is:

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

(a) Write π in cycle notation.

(b) What is $\pi \circ \pi$? Write it both in cycle notation and in two-line notation. Is it the identity permutation?

(c) What are the permutations π^n for $n \in \{3, 4, 5, 6, 7\}$? Use the cycle notation, two-line notation or one-line notation, whichever is convenient.

(d) Did you encounter the identity permutation in the previous part? If you did, can you now easily name a positive integer n such that $\pi^n = \pi^{-1}$?

Solution.

(a)

$$(1\ 2)(3\ 4)(5\ 7\ 6)$$

(b) In cycle notation

$$\begin{aligned}\pi \circ \pi =&(1\ 2)(3\ 4)(5\ 7\ 6)(1\ 2)(3\ 4)(5\ 7\ 6)\\ =&(1\ 2)(1\ 2)(3\ 4)(3\ 4)(5\ 7\ 6)(5\ 7\ 6)\\ =&(5\ 7\ 6)(5\ 7\ 6)\\ =&(5\ 6\ 7),\end{aligned}$$

which in two-line notation is

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 6 & 7 & 5 & 8 \end{pmatrix}$$

(c)

$n \equiv 1$	$(\text{mod } 6)$	$(1\ 2)(3\ 4)(5\ 7\ 6)$
$n \equiv 2$	$(\text{mod } 6)$	$(5\ 6\ 7)$
$n \equiv 3$	$(\text{mod } 6)$	$(1\ 2)(3\ 4)$
$n \equiv 4$	$(\text{mod } 6)$	$(5\ 7\ 6)$
$n \equiv 5$	$(\text{mod } 6)$	$(1\ 2)(3\ 4)(5\ 6\ 7)$
$n \equiv 6$	$(\text{mod } 6)$	identity

(d)

$$\begin{aligned}\pi^{-1} &= (6\ 7\ 5)(4\ 3)(2\ 1)\\ &= (1\ 2)(3\ 4)(5\ 6\ 7) = \pi^5\end{aligned}$$

$$n = 5$$

5A3 (Combination lock) Consider a combination lock which has two dials, each having ten positions labeled $0, 1, 2, \ldots, 9$ in order. A position of the lock is a pair $(a, b) \in S^2$, where a is the position of the first dial, and b that of the second dial, and $S = \{0, 1, 2, \ldots, 9\}$.

Because of the mechanism, the dials can only be rotated forward, to the next bigger integer, and from 9 to 0. Also the two dials are somehow stuck. The first dial can be rotated on its own, but if the second dial is rotated, it drags the first dial along, so that both move one step forward. So there are two possible functions that can be applied to change the lock position:

$$\begin{aligned}&f : (S \times S) \to (S \times S) : f(a, b) = ((a + 1) \bmod 10,\ b)\\ &g : (S \times S) \to (S \times S) : g(a, b) = ((a + 1) \bmod 10,\ (b + 1) \bmod 10)\end{aligned}$$

The operation $(x \bmod 10)$ means taking the remainder of x when dividing by ten (= taking the last digit), so $(9 + 1) \bmod 10 = 10 \bmod 10 = 0$.

(a) From position $(5, 3)$, how many and what positions can be reached by repeated application of f?

(b) From position $(5, 3)$, how many and what positions can be reached by repeated application of g?

(c) From position $(5, 3)$, is it possible to reach position $(4, 5)$ by some sequence of applications of f and g? If yes, how?

(d) (OPTIONAL, not required, no points) Is it possible to reach any position from any position by applying f and g in some sequence?

Solution.

(a) 10 different positions

$$\{\ (x, 3) \mid x \in S\ \}$$

(b) 10 different positions

$$\{\ ((5 + x) \bmod 10,\ (3 + x) \bmod 10) \mid x \in S\ \}$$

(c) Yes,

$$(4, 5) = g^2(f^7(5, 3))$$

(d) Yes, g can be used to cycle through all $y \in S$ in (x, y), and once y is fixed, f can be used to cycle through all $x \in S$ in (x, y) without affecting y.

5A4 (Square symmetries) We have four points marked on the plane:

$$A = (-1, 1), \quad B = (1, 1), \quad C = (1, -1), \quad D = (-1, -1).$$

Draw a picture and observe that they are corners of a square. We are interested in possible movements of the square, such that the corners change places, but the square itself as a geometric figure stays the same. We model this by *permutations* of the four corners. We define some "elementary" operations as permutations in cycle notation:

$$R = (ABCD)$$
$$H = (AB)(CD)$$
$$V = (AD)(BC)$$

We think of R of rotating the square clockwise by 90 degrees, so that the corner that is at point A moves to point B, the corner that is at point B moves to C, and so on.

(a) How many and what permutations of the corners can be obtained by a repeated application of R only? List them and explain in words. Remember that the identity is also a permutation.

(b) How many and what permutations of the corners can be obtained by a repeated application of H only? List them and explain in words.

(c) What are $H \circ V$ and $V \circ H$? Are they the same?

(d) What are $H \circ R$ and $R \circ H$? Are they the same?

(e) Is $H \circ V$ equal to R^n for some n?

(f) Prove that V can be done by some composition of R and H (in some order and perhaps many times).

(g) (OPTIONAL, not required, no points) How many and what permutations can be obtained as compositions of R and H (each can be used zero or more times, and in any order you like)?

Solution.

(a) 4, rotate once, twice, thrice, and the fourth rotation returns to identity.

(b) 2, mirror image and identity, mirroring the mirror image again returns the identity.

(c) Yes,

$$\begin{bmatrix} A & B \\ D & C \end{bmatrix} \xrightarrow{V} \begin{bmatrix} D & C \\ A & B \end{bmatrix} \xrightarrow{H} \begin{bmatrix} C & D \\ B & A \end{bmatrix}$$

$$\begin{bmatrix} A & B \\ D & C \end{bmatrix} \xrightarrow{H} \begin{bmatrix} B & A \\ C & D \end{bmatrix} \xrightarrow{V} \begin{bmatrix} C & D \\ B & A \end{bmatrix}$$

(d) No,

$$\begin{bmatrix} A & B \\ D & C \end{bmatrix} \xrightarrow{R} \begin{bmatrix} D & A \\ C & B \end{bmatrix} \xrightarrow{H} \begin{bmatrix} A & D \\ B & C \end{bmatrix}$$

$$\begin{bmatrix} A & B \\ D & C \end{bmatrix} \xrightarrow{H} \begin{bmatrix} B & A \\ C & D \end{bmatrix} \xrightarrow{H} \begin{bmatrix} C & B \\ D & A \end{bmatrix}$$

(e) $H \circ V = R^2$

(f)

$$\begin{aligned} HH &= \text{identity} \longleftrightarrow H = H^{-1} \\ VV &= \text{identity} \longleftrightarrow V = V^{-1} \\ R^4 &= \text{identity} \longleftrightarrow R^2 = R^{-2} \end{aligned}$$

$$HV = R^2 \longleftrightarrow H^{-1}HV = H^{-1}R^2 \longleftrightarrow V = HR^2$$

also

$$V = HR^2 \longleftrightarrow V^{-1} = (HR^2)^{-1} \longleftrightarrow V^{-1} = R^{-2}H^{-1} \longleftrightarrow V = R^2H$$

(g) 8, 4 rotations and a mirror for each

5A5 (Infinite permutations) In the lecture material, a *permutation* was defined simply as a bijection from some set A to itself. Most commonly permutations are studied in finite sets, but nothing really stops us from studying permutations of infinite sets.

Which of the following functions are permutations? For those that are permutations, find some positive integer n such that f^n is the identity function. The notation f^n means repeated composition here. If there is no such number, explain why. Try to make n as small as possible, if there are many choices.

(a) $f : \mathbb{R} \to \mathbb{R} : f(x) = -x$

(b) $f : \mathbb{N} \to \mathbb{N} : f(x) = x + 2$

(c) $f : \mathbb{Z} \to \mathbb{Z} : f(x) = x + 2$

(d) $f : \mathbb{N} \to \mathbb{N} : f(x) = \begin{cases} x + 1 & \text{if } x \text{ is even} \\ x - 1 & \text{if } x \text{ is odd} \end{cases}$

(e) $f : (\mathbb{R} \times \mathbb{R}) \to (\mathbb{R} \times \mathbb{R}) : f(x, y) = (y, x)$

(f) $f : (\mathbb{R} \times \mathbb{R}) \to (\mathbb{R} \times \mathbb{R}) : f(x, y) = (-y, x)$

(g) If we start from point $p = (3, 1)$, what are $(f^n)(p)$ for $n = 1, 2, 3, 4$, using the function from (e)?

(h) If we start from point $p = (3, 1)$, what are $(f^n)(p)$ for $n = 1, 2, 3, 4$, using the function from (f)?

(i) Explain in words what the functions from (e) and (f) do to points in the plane.

(j) (OPTIONAL, not required, no points) How would you express the functions from (c) and (d) in cycle notation? You can use the "three dots" liberally, don't worry too much about mathematical precision here — try to express the idea.

Solution.

(a) f is a permutation as it is a bijection from a set onto itself. $f^2(x) = -(-x) = x$, $n = 2$

(b) f is not a permutation, the smallest two values of x are never function values, which means f is not a bijection and therefore also not a permutation.

(c) f i a permutation as it is a bijection from a set onto itself. However there is no n for which f^n would equal identity, $f^n(x) = x + 2n \neq x$ for all non-zero $n \in \mathbb{Z}$.

(d) f is a permutation as it is a bijection from a set onto itself. $f^2(x) = x \pm 1 \mp 1 = x$, $n = 2$

(e) f is a permutation as it is a bijection from a set onto itself. $f^2(x, y) = f(y, x) = (x, y)$, $n = 2$

(f) f is a permutation as it is a bijection from a set onto itself. $f^4(x, y) = f^3(-y, x) = f^2(-x, -y) = f(y, -x) = (x, y)$, $n = 4$

(g)

$$\begin{aligned}
f^1(3, 1) &= (1, 3)\\
f^2(3, 1) &= (3, 1)\\
f^3(3, 1) &= (1, 3)\\
f^4(3, 1) &= (3, 1)
\end{aligned}$$

(h)

$$\begin{aligned}
f^1(3, 1) &= (-1, 3)\\
f^2(3, 1) &= (-3, -1)\\
f^3(3, 1) &= (1, -3)\\
f^4(3, 1) &= (3, 1)
\end{aligned}$$

(i) $f(x, y) = (y, x)$ mirrors all points of the plane along the line $x = y$. $f(x, y) = (-y, x)$ rotates the plane around the origin $\frac{\pi}{2}$ radians.

Analogy for $\frac{\pi}{2}$ rotation with complex analysis:

$$i(x + iy) = -y + ix$$

(j) (Optional part.) The function in (c) maps every integer two steps forward, so all evens map to evens, and all odds map to odds. We might write this as

$$(\ldots, -4, -2, 0, 2, 4, \ldots)\ (\ldots, -3, -1, 1, 3, 5, \ldots),$$

saying that the permutation has two “cycles”, both of infinite length. Every integer belongs to one of these cycles. But if you apply f over and over, you never return to where you started (which would happen in a finite cycle).

The function in (d) swaps consecutive natural numbers. We might write it as

$$(0\ 1)(2\ 3)(4\ 5)(6\ 7)\ldots$$

Now the cycles are finite (length two) but there are infinitely many. Every natural number belongs to one cycle. If you start from 4 and apply f repeatedly, you get $4 \mapsto 5 \mapsto 4 \mapsto 5 \mapsto \ldots$

5A6 (Shift cipher) The following table lists the 26 English letters in alphabetical order, and numbers indicating their positions.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

The *shift cipher* is a simple text encryption method, already known to the ancient Romans. First we specify a key $s \in \mathbb{Z}$. Then, to each letter in a text, we apply the same function f_s, which replaces the letter with the letter that is s steps to the right in the alphabet, wrapping around at the end (you can think of the letters being arranged around a circle). A negative key means shifting to the left. With key 1, PIZZA becomes QJAAB, and with key -1, PIZZA becomes OHYYZ.

(a) How many different shift ciphers exist? We said s can be any integer, but recall that two functions f, g are considered equal if $f(x) = g(x)$ for every x in the domain.

(b) Express f_3 as a permutation of letters, in cycle notation. How many cycles does it have and how long are they? This is called the *Caesar cipher*. Julius Caesar is reported to have used it.

(c) Express f_{13} as a permutation of letters, in cycle notation. How many cycles does it have and how long are they? This is called the *ROT13 cipher*.

(d) What happens to a text if you apply ROT13 twice? If the encrypted text is TBBQ, what is the original text?

(e) If f_s is a shift cipher, is its inverse function $(f_s)^{-1}$ also a shift cipher?

(f) If you apply several shift ciphers (same or different) in sequence, is the result again a shift cipher? For example, what is $(f_4 \circ f_6 \circ f_3)$?

Solution.

(a) 26, or 25 and the identity. $f_s = f_{s+26}$

(b)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3

or

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

cycle notation:

1 4 7 10 13 16 19 22 25 2 5 8 11 14 17 20 23 26 3 6 9 12 15 18 21 23

or

A D G J M P S V Y B E H K N Q T W Z C F I L O R U Y

One cycle of length 26.

(c)

$$(1\ 14)(2\ 15)(3\ 16)(4\ 17)(5\ 18)(6\ 19)(7\ 20)(8\ 21)(9\ 22)(10\ 23)(11\ 24)(12\ 25)(13\ 26)$$

or

$$(AN)(BO)(CP)(DQ)(ER)(FS)(GT)(HU)(IV)(JW)(KX)(LY)(MZ)$$

13 cycles of length 2.

(d) Applying ROT13 twice yields the original text as all cycle are of length 2, $f_{13}^2 = f_{13}$. Applying ROT13 to "TBBQ"results in the original message, which is "GOOD".

(e) Yes, if f_s is a shift cipher, then $(f_s)^{-1}$ is also a shift cipher.

f_s is a permutation and therefore a bijection and bijections have inverses.

$$\begin{aligned} f_s(x) = y,\ x = f_s^{-1}(y) & \\ y \equiv f_s(x) \equiv x + s & \qquad \text{mod } 26 \\ y - s \equiv x & \qquad \text{mod } 26 \end{aligned}$$

and now we have $y - s \bmod 26$, which is $f_{-s}(y)$ and it is congruent to x, which is $(f_s)^{-1}(y)$, and therefore

$$(f_s)^{-1}(y) = f_{-s}(y)$$

(f) Applying multiple shift ciphers results in another shift cipher.

$$f_s(f_t(x)) = f_s(x+t) = x+t+s = f_{s+t}(x)$$

and a simple induction proves that this can be repeated to a combined function of any number of shift ciphers.

$$f_4 \circ f_6 \circ f_3 = f_{3+6+4} = f_{13}$$

The challenge problem is worth an extra point.

5A7 (** Challenge: Cryptanalysis) Mr. Doofus, a secret agent, is sending a message his friend. He wants the message to be extra safe, so he applies the Caesar cipher (see the previous problem) many times, and the final result is FYNNWCYQRCP.

His friend, Smart Alec, receives this encrypted message. Alec knows that Mr. Doofus always uses the Caesar cipher, but does not know how many times it was applied. Being an expert cryptanalyst, Alec guesses that the second letter in the original text is probably one of the five vowels AEIOU (this is true in more than half of the words in English). Assuming this is true, Alec may be able to reverse the (unknown) encryption and recover the original message with a relatively small number of attempts.

What is the original message?

Hint: There are different methods for doing this. One option is to use a computer and try many different alternatives, until something resembling English is found. Another option is to exploit Alec's guess about the second letter being a vowel. With this method, a manual (non-computer) solution is probably feasible.

Solution. Let's attempt a manual solution using Alec's vowel guess. From the previous problem, we know that if Doofus applies Caesar several times, the result is again just a shift cipher.[1] If the Caesar chipher f_3 is applied twice,

[1] Which means his method is not very secure, since there are after all only 26 different shift ciphers, including the identity. Anyone could just try deciphering the text with 26 different keys. This could be done manually, with some work, or easily with a computer.

the result is f_6. If it is applied k times, the result is f_{3k}. To inverse Doofus's cipher, we need to apply f_{-3k} with some $k \in \mathbb{N}$.

Looking at the second letter of the ciphertext, Y, we apply successive inverse Caesar ciphers (f_{-3}), that is, move three positions left on each step:

$$Y \mapsto V \mapsto S \mapsto P \mapsto M \mapsto J \mapsto G \mapsto D \mapsto A.$$

Here, after 8 steps we found a vowel the first time. If Doofus applied Caesar 8 times, he was performing $f_{3\cdot 8} = f_{24}$, which is in fact the same as f_{-2}. The inverse would be $f_{-24} = f_2$, which maps $Y \mapsto A$.

Let's see what the proposed inverse f_2 does to some other letters in the ciphertext:

$$\begin{aligned} F &\mapsto H \\ Y &\mapsto A \\ N &\mapsto P \\ N &\mapsto P \\ W &\mapsto Y \end{aligned}$$

It is looking good, so we decide to go on for the full text (you can do the rest).

If this attempt were not successful, we could continue successive applications of f_{-3} on the second letter until the text begins in a plausible way. After two more steps we would hit U, but then the plaintext would begin BUJJS. After another two steps we would hit O, and the plaintext would begin VODDM.

This is just one possible method of breaking the cipher, and you may have thought of a different method. Real cryptanalysis uses various mathematical and linguistic methods (mathematics tells how texts change under encryption, and linguistics tells what the original text might possibly be). Also the encryption methods used these days are usually a bit more sopisticated than in Caesar's times.