The probability of generating the symmetric group with a commutator condition

David Zmiaikou[1]

Department of Mathematics, University Paris-Sud, 91400 Orsay, France

August 31, 2012

[1]Research partially supported by the Balzan Research Project of J. Palis

Abstract

Let $\mathcal{B}(n)$ be the set of pairs of permutations from the symmetric group of degree n with a 3-cycle commutator, and let $\mathcal{A}(n)$ be the set of those pairs which generate the symmetric or the alternating group of degree n. We find effective formulas for calculating the cardinalities of both sets. More precisely, we show that $\#\mathcal{B}(n)/n!$ is a discrete convolution of the partition function and a linear combination of divisor functions, while $\#\mathcal{A}(n)/n!$ is the product of a polynomial and Jordan's totient function. In particular, it follows that the probability that a pair of random permutations with a 3-cycle commutator generates the symmetric or the alternating group of degree n tends to zero as n tends to infinity, which makes a contrast with Dixon's classical result.

Key elements of our proofs are Jordan's theorem from the 19th century, a formula by Ramanujan from the 20th century and a technique of square-tiled surfaces developed by French mathematicians Lelièvre and Royer [11] in the beginning of the 21st century. This paper uses and highlights elegant connections between algebra, geometry, and number theory.

Contents

Notation **2**

Introduction **3**

1 General remarks **4**

2 The case of a cycle of maximal length **6**
- 2.1 A formula for $\#\mathcal{B}_1(n)$ . . . 7
- 2.2 A formula for $\#\mathcal{A}_1(n)$ . . . 7

3 The case of an arbitrary cycle **12**
- 3.1 A formula for $\#\mathcal{B}_2(n)$ . . . 12
- 3.2 A formula for $\#\mathcal{A}_2(n)$ . . . 14

4 The case of an arbitrary permutation **16**
- 4.1 The number of all pairs: a formula for $\#\mathcal{B}(n)$ . . . 16
- 4.2 The number of primitive pairs: a formula for $\#\mathcal{A}(n)$ . . . 23

A Background in number theory and permutation groups **37**
- A.1 Arithmetic functions . . . 37
- A.2 Partitions of a positive integer . . . 41
- A.3 Permutation groups . . . 42
- A.4 Representations of the symmetric group . . . 47
- A.5 Square-tiled surfaces . . . 51
- A.6 Lattices in $\mathbb{R}^2$ . . . 51
- A.7 Several useful sums . . . 53

B Programs (Sage) **54**
- B.1 Calculating $\#\mathcal{A}(n)$ and $\#\mathcal{B}(n)$ by Theorem A . . . 54
- B.2 Calculating $\#\mathcal{A}_1(n)$, $\#\mathcal{B}_1(n)$, $\#\mathcal{A}_2(n)$ and $\#\mathcal{B}_2(n)$ by Theorem B . . . 54
- B.3 The table for the first program . . . 55
- B.4 The table for the second program . . . 59

References **63**

Notation

$\mathbb{N} = \{1, 2, 3, \cdots\}$	set of natural numbers (positive integers)
$\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$	extended set of positive integers
$\mathbb{Z}$, $\mathbb{Q}$	sets of integer and rational numbers
$\mathbb{R}$, $\mathbb{R}^2$	real line and real plane
$[a, b[$, $]a, b]$	semi-open intervals of real numbers from a to b
$C_n^k = \frac{n!}{k!(n-k)!}$	binomial coefficient
$a \wedge b$	greatest common divisor of a and b
$a \bmod b$	remainder (residue) after the division of a by b
$[\![a, b]\!]$	set of integers in an interval $[a, b]$
$\liminf a_n$, $\limsup a_n$	lower and upper limits of a sequence (a_n)
$\mathrm{tr}(A)$, $\det(A)$	trace and determinant of a matrix A
$\mathrm{SL}_2(\mathbb{Z})$	group of integer 2×2 matrices with determinant 1
$\mathrm{GL}_d(\mathbb{C})$	group of complex $d \times d$ matrices with nonzero determinant
χ_ρ	character of a representation ρ
$f \cdot g$	product of two functions, $(f \cdot g)(n) = f(n)g(n)$
$f \vartriangle g$	discrete convolution of two functions, $(f \vartriangle g)(n) = \sum_{k=1}^{n-1} f(k)g(n-k)$
$f * g$	Dirichlet convolution of two functions, $(f * g)(n) = \sum_{d\mid n} f(d)g(n/d)$
$\mathcal{F}$	set of all arithmetic functions
$\mathcal{F}^*$	set of arithmetic functions different from zero at 1
$\mathcal{F}_{\mathrm{mult}}$	set of multiplicative arithmetic functions
$\varepsilon(n)$	trivial function, $\varepsilon(1) = 1$ and $\varepsilon(n) = 0$ for $n > 1$
$\mathbb{1}(n)$	constant function, $\mathbb{1}(n) \equiv 1$
$\mathrm{id}(n)$	identical function, $\mathrm{id}(n) = n$
$\mathrm{id}_k(n)$	power function of order k, $\mathrm{id}_k(n) = n^k$
$\mu(n)$	Möbius function
$\tau(n)$	number of divisors of n
$\sigma(n)$	sum of divisors of n
$\sigma_k(n)$	sigma-function of order k (sum of k^{th} powers of the divisors of n)
$\phi(n)$	Euler's totient function (number of integers from 1 to n coprime with n)
$J_k(n)$	Jordan's totient function of order $k > 0$
$P(n)$	number of partitions of a positive integer n (partition function)
$\mathscr{P}(n)$	set of partitions of n
$\#M$ or $\lvert M\rvert$	cardinality of a set M
$M \hookrightarrow L$	injection from a set M to a set L
$M \twoheadrightarrow L$	surjection from a set M to a set L
$M \times L$	Cartesian product of sets M and L
s^{-1}	inverse permutation to s
$s \circ t$ or st	composition of two permutations s and t
$[s, t] = sts^{-1}t^{-1}$	commutator of two permutations s and t
$Alt(M)$, $Sym(M)$	alternating and symmetric groups of a set M
A_n, S_n	alternating and symmetric groups of the set $\{1, 2, \dots, n\}$
$\langle s, t\rangle$	group generated by s and t
G_x	stabilizer of a point x for an action of a group G
$\mathrm{supp}(s)$, $\mathrm{fix}(s)$	support of a permutation s and set of points fixed by s
$\mathsf{Graph}(s_1, \dots, s_g)$	graph of permutations $s_1, \dots, s_g$
$\mathsf{type}(s)$	cycle type of a permutation s
$\mathsf{flag}(s)$	flag of a permutation s
$\mathbb{d}_s : [\![1, n]\!]^2 \to \mathbb{N}_\infty$	s-distance on the set $[\![1, n]\!]$, where $s \in S_n$
$O_{s,t}$	square-tiled surface corresponding to a pair of permutations (s, t)

Introduction

In 1892, Netto conjectured that almost all pairs of permutations will generate the symmetric or the alternating group. 76 years passed before the theorem was finally proved by Dixon. This paper investigates a refinement of Netto's conjecture.

Denote by $\mathcal{B}(n)$ the set of pairs of permutations from S_n with a 3-cycle commutator, and let $\mathcal{A}(n)$ be the set of those pairs which generate the symmetric or the alternating group of degree n:

$$\mathcal{B}(n) = \{(s,t) \in S_n \times S_n \mid [s,t] \text{ is a 3-cycle}\},$$

$$\mathcal{A}(n) = \{(s,t) \in \mathcal{B}(n) \mid \langle s,t \rangle = A_n \text{ or } S_n\}.$$

We find the cardinalities of these sets, and show that the probability that a pair of permutations with a 3-cycle commutator generates A_n or S_n tends to zero as $n \to \infty$.

Theorem A. (*cf.* Theorems 1, 2 and Corollary 7)
The following relations hold for any $n > 2$:

$$\#\mathcal{B}(n) = \frac{3}{8}\left(\sum_{k=1}^{n} \sigma_3(k)P(n-k) - 2\sum_{k=1}^{n} k\sigma_1(k)P(n-k) + nP(n)\right)n!,$$

$$\#\mathcal{A}(n) = \frac{3}{8}(n-2)J_2(n)\, n!,$$

where $\sigma_\ell(n)$ is the sum of the ℓ^{th} powers of the positive divisors of n, $J_\ell(n)$ is Jordan's totient function of order ℓ, and $P(n)$ is the partition function.

In particular, the probability $\#\mathcal{A}(n)/\#\mathcal{B}(n)$ tends to zero as n tends to infinity.

We also consider intermediate sets

$$\mathcal{B}_1(n) = \{(s,t) \in S_n \times S_n \mid [s,t] = \text{3-cycle},\ s = n\text{-cycle}\},$$

$$\mathcal{A}_1(n) = \{(s,t) \in \mathcal{B}_1(n) \mid \langle s,t \rangle = A_n \text{ or } S_n\},$$

$$\mathcal{B}_2(n) = \{(s,t) \in S_n \times S_n \mid [s,t] = \text{3-cycle},\ s = \text{arbitrary cycle}\},$$

$$\mathcal{A}_2(n) = \{(s,t) \in \mathcal{B}_2(n) \mid \langle s,t \rangle = A_n \text{ or } S_n\}$$

and prove the following theorem:

Theorem B. (*cf.* Propositions 1, 2, 3, 4 and Corollaries 2, 3)
For any natural $n > 2$, one has the formulas:

$$\#\mathcal{B}_1(n) = C_n^3\, n!, \qquad \#\mathcal{B}_2(n) = \frac{1}{24}(n-1)(n-2)(n^2+5n+12)\, n!,$$

$$\#\mathcal{A}_1(n) = \frac{n}{6}\Big(J_2(n) - 3J_1(n)\Big)n!, \qquad \#\mathcal{A}_2(n) = \frac{n}{6}\Big(J_2(n) - 3J_1(n)\Big)n! + \frac{(n+1)(n-2)}{2}n!.$$

In particular, for the probabilities $p_1(n) = \#\mathcal{A}_1(n)/\#\mathcal{B}_1(n)$ and $p_2(n) = \#\mathcal{A}_2(n)/\#\mathcal{B}_2(n)$ we obtain the lower and the upper limits:

$$\liminf p_1(n) = 6/\pi^2, \qquad \liminf n \cdot p_2(n) = 24/\pi^2,$$
$$\limsup p_1(n) = 1 \qquad \limsup n \cdot p_2(n) = 4.$$

1 General remarks

Denote by $[\![a,b]\!]$ the set of integer from a to b. Introduce the extended set of positive integers $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$. Recall that any permutation set $[\![1,n]\!]$ decomposes into a product of disjoint cycles (*cf.* Lemma A.1).

Definition. Let $s \in S_n$ be a permutation. The ***s*-distance** on the set $[\![1,n]\!]$ is defined to be the function $\mathbb{d}_s : [\![1,n]\!]^2 \to \mathbb{N}_\infty$ such that

$$\mathbb{d}_s(x,y) = \begin{cases} \min\left\{d \in \mathbb{N} \;\middle|\; s^d(x) = y\right\}, & \text{if } x \text{ and } y \text{ lie in the same cycle of } s\,; \\ \infty, & \text{otherwise.} \end{cases} \tag{1}$$

In particular, the s-distance $\mathbb{d}_s(x,x)$ is equal to the length of the cycle containing x.

For instance, for the permutation $s = (1\,2\,3\,4)(7\,8\,9)$ we have

$$\mathbb{d}_s(1,4) = 3, \quad \mathbb{d}_s(1,5) = \mathbb{d}_s(1,8) = \infty, \quad \mathbb{d}_s(6,6) = 1, \quad \mathbb{d}_s(7,8) = 1, \quad \mathbb{d}_s(9,9) = 3.$$

Note that the function $\mathbb{d}_s$ is not symmetric. In the example above, $\mathbb{d}_s(1,4) = 3$ but $\mathbb{d}_s(4,1) = 1$. Evidently, two integers x and y lie in the same cycle of s if and only if

$$\mathbb{d}_s(x,y) + \mathbb{d}_s(y,x) = \mathbb{d}_s(x,x).$$

Lemma 1. *Suppose that the commutator of two permutations s and t from S_n is a 3-cycle, $[s,t] = (z\;y\;x)$. Then one of the following holds:*

(a) *all three numbers x, y, z lie in the same cycle of s in the given order, that is*

$$\mathbb{d}_s(x,y) + \mathbb{d}_s(y,z) + \mathbb{d}_s(z,x) = \mathbb{d}_s(x,x);$$

(b) *two numbers (say x and y) lie in the same cycle of s, and the third one (z) lies in another cycle such that $\mathbb{d}_s(z,z) = \mathbb{d}_s(y,x)$.*

Proof. The equality $sts^{-1}t^{-1} = (z\;y\;x)$ can be re-written as

$$(x\;y\;z)s = tst^{-1} \tag{2}$$

when one multiplies the former equality by the permutation $(ts^{-1}t^{-1})^{-1} = tst^{-1}$ from the right and by $(z\;y\;x)^{-1} = (x\;y\;z)$ from the left. From this relation follows that the permutations $(x\;y\;z)s$ and s are conjugate – they have the same cycle type (*cf.* the section A.3 of Appendix).

Suppose that the numbers $x = x_1$, $y = y_1$, $z = z_1$ lie in distinct cycles of s, that is that s is the following product of permutation with disjoint supports:

$$s = (x_1\;\ldots\;x_a)(y_1\;\ldots\;y_b)(z_1\;\ldots\;z_c)\,u\,,$$

Then the permutation

$$(x_1\;y_1\;z_1)s = (x_1\;\ldots\;x_a\;y_1\;\ldots\;y_b\;z_1\;\ldots\;z_c)\,u$$

is not conjugate to s, which contradicts the condition (2). Thus, either all three numbers x, y, z lie in the same cycle of s, or two of them lie in one cycle of the permutation s and the third number – in another cycle.

Consider the case (a). Up to a cyclic permutation, the set of three elements can be ordered in two ways: x, y, z or z, y, x. If the numbers x, y, z lie in some cycle s in the inverse order, that is if

$$s = (z_1\;\ldots\;z_c\;y_1\;\ldots\;y_b\;x_1\;\ldots\;x_a)\,u\,,$$

then the permutation

$$(x_1\ y_1\ z_1)s = (x_1\ \dots\ x_a)(y_1\ \dots\ y_b)(z_1\ \dots\ z_c)\,u$$

is not conjugate to s, which is false. Therefore, the numbers x, y, z must be in the given order.

Consider the case (b), where s can be presented as the following product of permutations with disjoint supports:

$$s = (z_1\ \dots\ z_c)(y_1\ \dots\ y_b\ x_1\ \dots\ x_a)\,u\,.$$

Then, since the permutation

$$(x_1\ y_1\ z_1)s = (y_1\ \dots\ y_b)(z_1\ \dots\ z_c\ x_1\ \dots\ x_a)\,u$$

must be conjugate to s, we obtain $c = b$, that is $\mathbb{d}_s(z,z) = \mathbb{d}_s(y,x)$. □

Consider a pair of permutations $(s,t) \in S_n \times S_n$ such that $[s,t] = (z_1\ y_1\ x_1)$. Suppose that the permutation group $G = \langle s,t\rangle$ is transitive. Then by means of Lemma 1, one can get a simple description of the *connected* square-tiled surface $O(s,t)$ defined in the section A.5 of Appendix. It was first obtained by Zorich (*cf.* the monograph [19]). More precisely, there can be only two following situations:

(a) The permutation s is a product of k disjoint cycles of length n/k,

$$s = u_1 u_2 \cdots u_k\,,$$

moreover, one of the cycles, say u_1, is presentable as $u_1 = (x_1\ \dots\ x_a\ y_1\ \dots\ y_b\ z_1\ \dots\ z_c)$ so that

$$(x_1\ y_1\ z_1)s = (x_1\ \dots\ x_a\ z_1\ \dots\ z_c\ y_1\ \dots\ y_b)\,u_2 \cdots u_k.$$

The permutation t is such that, when conjugating s, it sends the cycle u_i to the cycle u_{i+1} for any $i \in [\![1, k-1]\!]$, and the cycle u_k is sent to $(x_1\ \dots\ x_a\ z_1\ \dots\ z_c\ y_1\ \dots\ y_b)$.

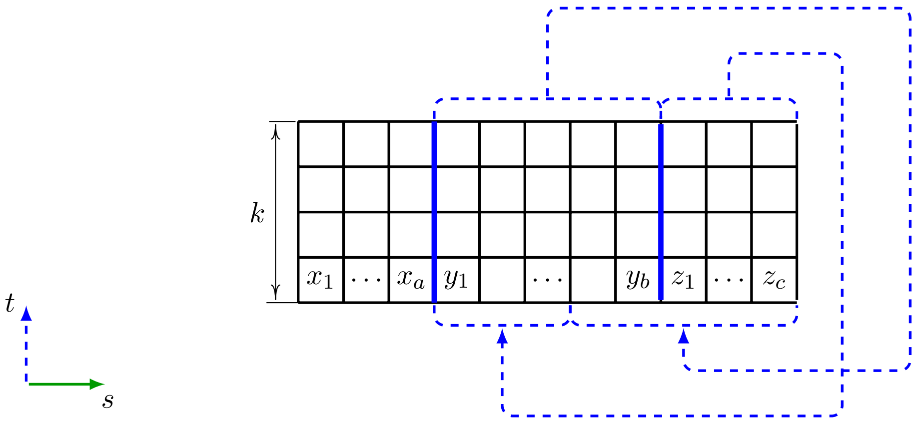

Figure 1: One-cylinder origami with parameters (k,a,b,c).

The square-tiled surface $O(s,t)$ is illustrated in Figure 1, where any two unmarked opposite sides are identified. It is called the **one-cylinder origami with parameters** (k,a,b,c).

(b) The permutation s is a product of a cycles of length k and b cycles of length ℓ,

$$s = u_1 \cdots u_a\, v_1 \cdots v_b\,, \qquad \text{where}\ \ k < \ell\ \ \text{and}\ \ ak + b\ell = n.$$

The cycle u_1 contains the point z_1, and the cycle v_1 contains the points y_1 and x_1. Moreover, the s-distance from y_1 to x_1 is equal to the length of the cycle u_1:

$$u_1 = (z_1\ \dots\ z_k) \qquad\qquad v_1 = (y_1\ \dots\ y_k\ x_1\ \dots\ x_{k-\ell}),$$

so that

$$(x_1\ y_1\ z_1)s = (y_1\ \dots\ y_k)\,u_2 \cdots u_a\,(z_1\ \dots\ z_k\ x_1\ \dots\ x_{k-\ell})\,v_2 \cdots v_b\,.$$

The permutation t conjugates s in the following way:

- the cycle u_i is sent to the cycle u_{i+1} for any $i \in [\![1, a-1]\!]$,
- the cycle v_j is sent to the cycle v_{j+1} for any $j \in [\![1, b-1]\!]$,
- the cycle u_a is sent to the cycle $(y_1\ \dots\ y_k)$,
- the cycle v_b is sent to the cycle $(z_1\ \dots\ z_k\ x_1\ \dots\ x_{k-\ell})$.

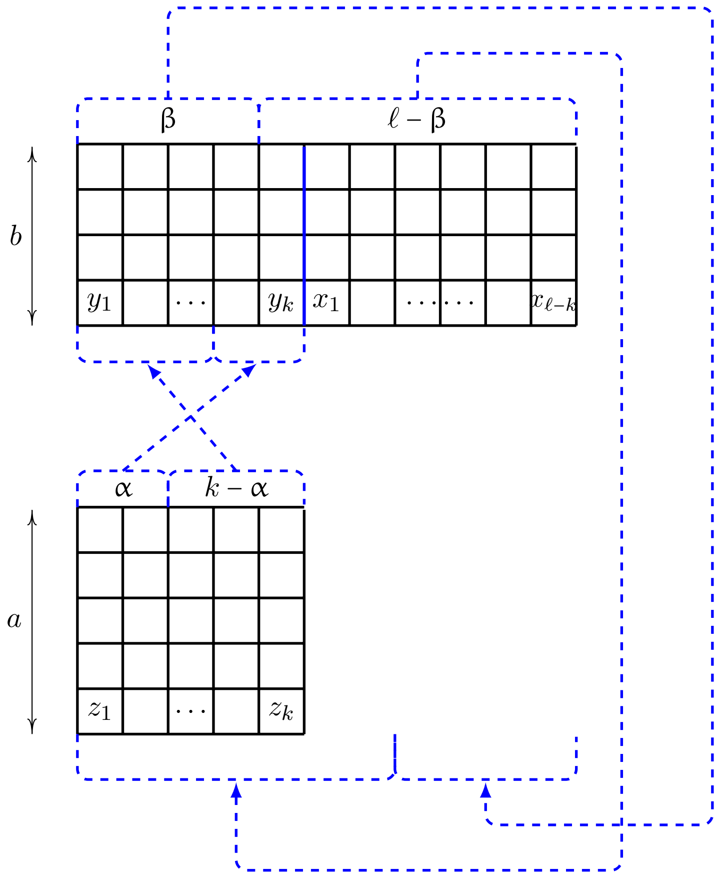

Figure 2: Two-cylinder origami with parameters $(a, b, k, \ell, \alpha, \beta)$.

The square-tiled surface $O(s,t)$ is illustrated in Figure 2, where any two unmarked opposite sides are identified. It has six parameters:

$$\textbf{heights } a, b \in \mathbb{N}, \quad \textbf{lengths } k < \ell \in \mathbb{N}, \quad \textbf{twists } \alpha \in [\![0, k-1]\!] \text{ and } \beta \in [\![0, \ell-1]\!].$$

Such a surface is called **two-cylinder with parameters** $(a, b, k, \ell, \alpha, \beta)$.

2 The case of a cycle of maximal length

In this section, we will be interested in the following set:

$$\mathcal{A}_1(n) = \{(s,t) \in S_n \times S_n \mid [s,t] \text{ is a 3-cycle, } s \text{ is an } n\text{-cycle, } \langle s,t \rangle = A_n \text{ or } S_n\},$$

$$\mathcal{B}_1(n) = \{(s,t) \in S_n \times S_n \mid [s,t] \text{ is a 3-cycle, } s \text{ is an } n\text{-cycle}\}.$$

2.1 A formula for $\#\mathcal{B}_1(n)$

Proposition 1. *The number of pairs of permutations $(s,t) \in S_n \times S_n$ such that the commutator $[s,t]$ is a 3-cycle and the permutation s is a cycle of length n, is equal to*

$$\#\mathcal{B}_1(n) = C_n^3\, n! \tag{3}$$

Proof. It follows from to Lemma 1, that for an n-cycle s, there exists a permutation $t \in S_n$ with condition $[s,t] = (z\ y\ x)$ if and only if the points x, y, z lie in the same cycle of s in the given order. Such a permutation t will be called an **allowed permutation for** s, and such a triple $(x,y,z) \in [\![1,n]\!]^3$ will be said to be an **allowed triple for** s. Herewith, we assume that the number x is less than y and z. It is clear that for any n-cycle s, the number of allowed triples is equal to the binomial coefficient $C_n^3 = \frac{1}{6}n(n-1)(n-2)$.

Remark that in order to find the cardinality of the set $\mathcal{B}_1(n)$, it is sufficient to calculate the number of allowed permutations t for some n-cycle s, say for $s_0 = (1\ 2\ \ldots\ n)$, and then multiply that number by the number of all n-cycles in S_n.

Further, for a fixed n-cycle s_0 and a fixed allowed triple (x,y,z), the number of all t such that

$$[s_0, t] = (z\ y\ x), \quad \text{that is} \quad t s_0 t^{-1} = (x\ y\ z)s_0,$$

is equal to the order of the centralizer $C_{S_n}(s_0)$ of the permutation s_0 in S_n. Indeed, the group S_n acts on its element via conjugation. As the permutations $(x\ y\ z)s_0$ and s_0 lie in the same orbit (they are both n-cycles), then the number of distinct t sending s_0 to $(x\ y\ z)s_0$ is equal to the number of distinct t which stabilize the cycle s_0 , that is $|C_{S_n}(s_0)|$.

We obtain

$$\begin{aligned}
\#\mathcal{B}_1(n) &= \#\{(s,t) \in S_n \times S_n \mid [s,t] = \text{3-cycle},\ s = n\text{-cycle}\}\\
&= \#\{s \in S_n \mid s = n\text{-cycle}\} \times \#\{t \in S_n \mid t \text{ allowed for } s_0 = (1\ 2\ \ldots\ n)\}\\
&= \#\{s \in S_n \mid s = n\text{-cycle}\} \times |C_{S_n}(s_0)|\\
&\qquad\qquad \times \#\left\{(x,y,z) \in [\![1,n]\!]^3 \mid \text{the triple } (x,y,z) \text{ is allowed for } s_0\right\}\\
&= n! \times C_n^3.
\end{aligned}$$

Here we used the fact that the set $\{s \in S_n \mid s = n\text{-cycle}\}$ is the orbit of the permutation s_0 for the action of S_n via conjugation, and the centralizer $C_{S_n}(s_0)$ is the stabilizer of the permutation s_0. In particular, we have $\#\{s \in S_n \mid s = n\text{-cycle}\} \times |C_{S_n}(s_0)| = |S_n| = n!$. ☐

2.2 A formula for $\#\mathcal{A}_1(n)$

Let us now find the cardinality of the set $\mathcal{A}_1(n)$.

Lemma 2. *A one-cylinder square-tiled surface with parameters (k,a,b,c) is primitive if and only if $k = 1$ and $a \wedge b \wedge c = 1$.*

Proof. ($\Longrightarrow$) Let $O(s,t)$ be a *primitive* one-cylinder origami with parameters (k,a,b,c) as in Figure 1. By definition, its monodromy group $G = \langle s,t \rangle \subseteq S_n$ is primitive. The permutation s is a product of k disjoint cycles of length n/k,

$$s = u_1 u_2 \cdots u_k\,.$$

Consider the set of points Δ which are moved by the cycle u_1 :

$$\Delta = \operatorname{supp} u_1\,.$$

Let us prove that it is a block for the group G. Indeed, any permutation $w \in G$ can be presented as a word in the alphabet $\{s, t, s^{-1}, t^{-1}\}$:

$$w = s^{\varepsilon_1} t^{\varepsilon_2} \dots s^{\varepsilon_{\ell-1}} t^{\varepsilon_\ell}, \qquad \text{where } \ \varepsilon_i \in [\![-1, 1]\!],$$

since the group G is generated by the pair of permutations s and t. As

$$s(\operatorname{supp} u_j) = \operatorname{supp} u_j \qquad \text{and} \qquad t(\operatorname{supp} u_j) = \operatorname{supp} u_{j+1 \bmod k}$$

for each $j \in [\![1, k]\!]$, then the image of the set Δ under the action of w is equal to the support of one of the permutations $u_1, \dots, u_k$. In particular,

$$w(\Delta) = \Delta \quad \text{or} \quad w(\Delta) \cap \Delta = \varnothing\,,$$

from where Δ is a block for the group G. In view of the primitivity of G, we get that $\Delta = [\![1, n]\!]$, that is $k = 1$ and the permutation s is an n-cycle (*cf.* Figure 3):

$$s = (x_1 \ \dots \ x_a \ y_1 \ \dots \ y_b \ z_1 \ \dots \ z_c)\,.$$

Let us now show that the greatest common divisor $d = a \wedge b \wedge c$ equals 1. Consider the set

$$\Delta = \{x_d, x_{2d}, \dots, x_a, \ y_d, y_{2d}, \dots, y_b, \ z_d, z_{2d}, \dots, z_c\}\,,$$

which is subsequence of numbers in the cycle s with step d. Denote by

$$\Delta_j = \{x_{d+j}, x_{2d+j}, \dots, x_{a+j} = x_j, \ \ y_{d+j}, y_{2d+j}, \dots, y_{b+j} = y_j, \ \ z_{d+j}, z_{2d+j}, \dots, z_{c+j} = z_j\}$$

the j^{th} shift of the set Δ, where $j \in [\![1, d]\!]$. Then

$$s(\Delta_j) = \Delta_{j+1 \bmod d} \quad \text{and} \quad t(\Delta_j) = \Delta_j\,.$$

Hence, the image of the set Δ for the action of any permutation $w \in G$ (which can be expressed as a word on s and t) coincides with one of the shifts of Δ. In particular, $w(\Delta) = \Delta$ or $w(\Delta) \cap \Delta = \varnothing$, that is Δ is a block for the group G. Since G is primitive and Δ contains more than one element, then $\Delta = [\![1, n]\!]$, from where $d = 1$.

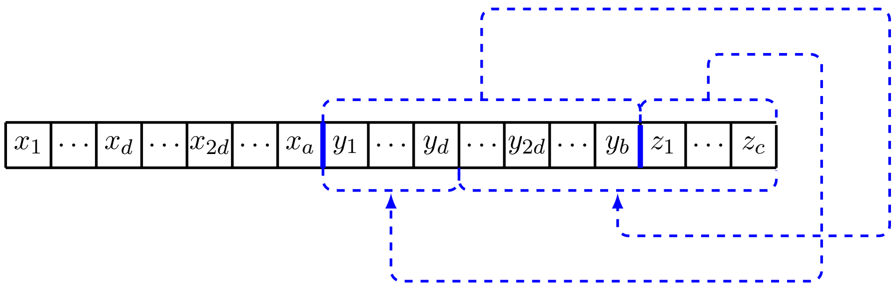

Figure 3: One-cylinder origami with parameters $(1, a, b, c)$.

$\Longleftarrow$ Conversely, consider a one-cylinder origami $O(s, t)$ with parameters $(1, a, b, c)$, where

$$s = (x_1 \ \dots \ x_a \ y_1 \ \dots \ y_b \ z_1 \ \dots \ z_c), \quad [s, t] = (z_1 \ y_1 \ x_1) \quad \text{and} \quad a \wedge b \wedge c = 1.$$

Without loss of generality, we can assume that $s = (1 \ 2 \ \dots \ n)$, $x_1 = 1$, $y_1 = a + 1$ and $z_1 = a + b + 1$. Let us show that the permutation group $G = \langle s, t \rangle$ is primitive. For this, consider an arbitrary block $\Delta \subseteq [\![1, n]\!]$ of the group G containing the point 1 and another point. Denote by d the least s-distance between the pairs of points from the block Δ. Choose a pair of points i and $i + d \pmod n$ from Δ, for which such distance is reached. Since $i + d \in \Delta \cap s^d(\Delta)$, then by definition of a block we have $\Delta = s^d(\Delta)$, and so the point $i + 2d$ also lies in Δ. By induction, we conclude that the block Δ contains the number

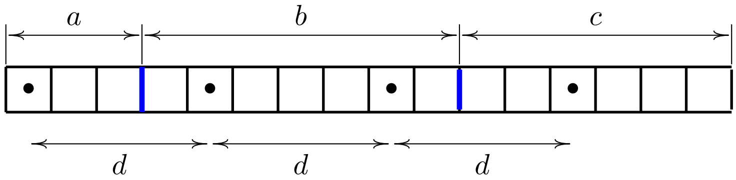

Figure 4: The marked points belong to the block Δ.

$i + \ell d \pmod n$ for any integer ℓ. As d is the least s-distance between points of the block and $1 \in \Delta$, then d divides n and

$$\Delta = \{1 + \ell d \bmod n \mid \ell \in \mathbb{Z}\}.$$

Let us also prove that d divides the numbers a, b and c. Indeed, divide a and $a+b$ by d:

$$a = \ell_1 d + r_1 \quad \text{and} \quad a + b = \ell_2 d + r_2$$

with remainders $r_1, r_2 \in [\![1, d]\!]$. Investigate the image $t(\Delta)$, *cf.* Figure 5. Since $1 \in \Delta \cap t(\Delta)$, then from the definition of a block follows that $t(\Delta) = \Delta$. Taking into account how the permutation t acts on

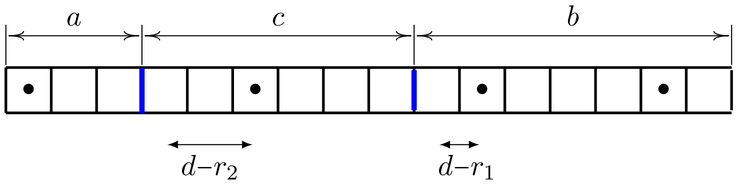

Figure 5: The marked points belong to the block $t(\Delta)$.

the set $[\![1, n]\!]$ and that d divides $a + b + c$, we obtain

$$d - r_1 = 0,$$

$$d - r_2 = d - r_1 .$$

Hence, $r_1 = r_2 = d$, from where d divides number a, $a + b$, $a + b + c$, and so the integers a, b, c as well. The last three numbers are coprime, implying that $d = 1$. ☐

Lemma 3. *Let d be a natural divisor of n. The number of triples (x, y, z) in the set $[\![1, n]\!]^3$ such that*

$$x < y < z, \quad d \mid y - x \quad \text{and} \quad d \mid z - y ,$$

is equal to $d \cdot C^3_{n/d}$.

Proof. Since the differences $y - x$ and $z - y$ are divisible by d, the numbers x, y, z are equal modulo d:

$$x = \alpha d + r, \quad y = \beta d + r, \quad z = \gamma d + r,$$

where $\alpha < \beta < \gamma \in [\![0, {}^{n}\!/\!_{d} - 1]\!]$ and $r \in [\![1, d]\!]$. There are exactly $C^3_{n/d}$ ways to choose a triple of coefficients (α, β, γ) and exactly d ways to choose a remainder r, which proves the statement. ☐

Lemma 4. *For any positive integer $n > 2$, the number of triples x, y, z in the set $[\![1, n]\!]$ such that*

$$x < y < z \quad \text{and} \quad (y - x) \wedge (z - y) \wedge n = 1 ,$$

equals $\frac{n}{6} J_2(n) - \frac{n}{2} J_1(n)$, *where $J_k(n)$ is Jordan's totient function of order k.*

Proof. We shall proceed by the inclusion-exclusion principle. There are C_n^3 triples $x < y < z$ in the interval $[\![1, n]\!]$. From this number one must subtract the number of triples such that $y - x$ and $z - y$ are simultaneously divisible by some prime divisor of n. After that, one must add the number of those triples, for which $y - x$ and $z - y$ are simultaneously divisible by some two *distinct* prime divisors of n, and so on. In the end, we will get

$$
\begin{aligned}
&\#\left\{(x,y,z) \in [\![1,n]\!]^3 \mid x < y < z,\ (y-x) \wedge (z-y) \wedge n = 1\right\} \\
&\quad = C_n^3 - \sum_{\substack{p|n \\ p \text{ prime}}} \left\{(x,y,z) \in [\![1,n]\!]^3 \mid x < y < z,\ p \text{ divides } y-x \text{ and } z-y\right\} \\
&\qquad + \sum_{\substack{p_1 p_2|n \\ p_1 \neq p_2 \text{ prime}}} \left\{(x,y,z) \in [\![1,n]\!]^3 \mid x < y < z,\ p_1 p_2 \text{ divides } y-x \text{ and } z-y\right\} \\
&\qquad - \sum_{\substack{p_1 p_2 p_3|n \\ p_1 \neq p_2 \neq p_3 \text{ prime}}} \left\{(x,y,z) \in [\![1,n]\!]^3 \mid x < y < z,\ p_1 p_2 p_3 \text{ divides } y-x \text{ and } z-y\right\} \\
&\qquad + \quad \dots \\
&\quad = \sum_{d|n} \mu(d) \left\{(x,y,z) \in [\![1,n]\!]^3 \mid x < y < z,\ d \text{ divides } y-x \text{ and } z-y\right\}.
\end{aligned}
$$

Due to Lemma 3, the last sum is equal to

$$
\sum_{d|n} \mu(d) d\, C_{n/d}^3 = \frac{1}{6} \sum_{d|n} \mu(d)\, n \left(\frac{n}{d} - 1\right)\left(\frac{n}{d} - 2\right) = \frac{n^3}{6} \sum_{d|n} \frac{\mu(d)}{d^2} - \frac{n^2}{2} \sum_{d|n} \frac{\mu(d)}{d} + \frac{n}{3} \sum_{d|n} \mu(d),
$$

and using the equality (A.16) for $k = 0, 1, 2$, we obtain the expression

$$
\frac{n^3}{6} \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right) - \frac{n^2}{2} \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) + \frac{n}{3} \times 0 = \frac{n}{6} J_2(n) - \frac{n}{2} J_1(n),
$$

which completes the proof. □

Proposition 2. *The number of pairs of permutations $(s,t) \in S_n \times S_n$ with a 3-cycle commutator, the permutation s being an n-cycle and which generate A_n or S_n, is equal to*

$$
\#\mathcal{A}_1(n) = \frac{n}{6}\Big(J_2(n) - 3J_1(n)\Big) n! \tag{4}
$$

Proof. We shall apply Jordan's theorem (Proposition A.7), Lemma 2, Lemma 1 and Lemma 4.

By Jordan's theorem, a pair of permutations $(s,t) \in S_n \times S_n$ with a 3-cycle commutator

$$
[s,t] = (z\ y\ x), \quad \text{that is} \quad tst^{-1} = (x\ y\ z)s, \tag{5}
$$

generates the alternating or the symmetric group of degree n if and only if the square-tiled surface $O(s,t)$ is primitive. If the permutation s is an n-cycle, then the surface $O(s,t)$ is one-cylinder. We conclude that according Lemma 2, the pair (s,t) belongs to the set $\mathcal{A}_1(n)$ if and only if the origami $O(s,t)$ is one-cylinder with parameters $(1, a, b, c)$, where $a \wedge b \wedge c = 1$.

A permutation $t \in S_n$ will be called **allowed for** s if $(s,t) \in \mathcal{A}_1(n)$. A triple of integers (x,y,z) from the set $[\![1,n]\!]^3$ will be said to be **allowed for** s if the relation (5) holds for some $t \in S_n$ and the pair (s,t) generates A_n or S_n. Herewith, we assume the the number x is less than y and z. From what

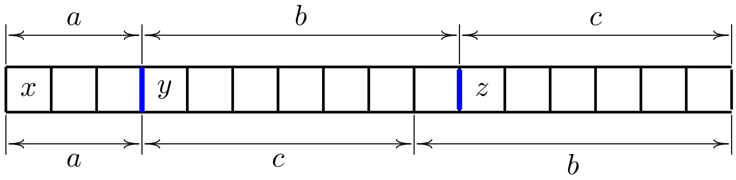

Figure 6: A primitive one-cylinder origami with parameters $(1, a, b, c)$.

was explained above and from Lemma 1 follows that a triple (x, y, z) is allowed for the permutation $s_0 = (1\,2\,\ldots\,n)$ if and only if

$$1 \leq x < y < z \leq n \quad \text{and} \quad (y - x) \wedge (z - y) \wedge (n - z + x) = 1, \tag{6}$$

since $\{y - x, z - y, n - z + x\} = \{a, b, c\}$. In Figure 6 we illustrated the case that $y - x = a$, $z - y = b$ and $n - z + x = c$. Since $n - z + x = n - (z - y) - (y - x)$, then any common divisor of the numbers $y - x$, $z - y$, $n - z + x$ divides also n, and conversely – any common divisor of $y - x$, $z - y$, n divides $n - z + x$. Therefore, the condition (6) can be re-written as

$$1 \leq x < y < z \leq n \quad \text{and} \quad (y - x) \wedge (z - y) \wedge n = 1.$$

The number of such triples has been found in Lemma 4.

Analogically to the proof of Proposition 1, we obtain

$$\begin{aligned}
\#\mathcal{A}_1(n) &= \#\{(s,t) \in S_n \times S_n \mid [s,t] = 3\text{-cycle},\ s = n\text{-cycle},\ \langle s,t\rangle = A_n \text{ or } S_n\} \\
&= \#\{s \in S_n \mid s = n\text{-cycle}\} \times \#\{t \in S_n \mid t \text{ is allowed for } s_0 = (1\,2\,\ldots\,n)\} \\
&= \#\{s \in S_n \mid s = n\text{-cycle}\} \times |C_{S_n}(s_0)| \\
&\qquad\qquad \times \#\left\{(x,y,z) \in [\![1,n]\!]^3 \mid \text{the triple } (x,y,z) \text{ is allowed for } s_0\right\} \\
&= n! \times \left(\frac{n}{6} J_2(n) - \frac{n}{2} J_1(n)\right),
\end{aligned}$$

as required. □

Corollary 1. *Let p be a prime number. For any p-cycle $s \in S_p$ and any permutation $t \in S_p$ such that the commutator $[s,t]$ is 3-cycle, the pair (s,t) must generate A_p or S_p.*

Proof. Indeed, according to Proposition 1 and 2

$$\begin{aligned}
\frac{\#\mathcal{B}(p)}{p!} &= \frac{p(p-1)(p-2)}{6}, \\
\frac{\#\mathcal{A}(p)}{p!} &= \frac{p}{6}\left(J_2(p) - 3J_1(p)\right) = \frac{p}{6}\left(p^2 - 1 - 3(p-1)\right) = \frac{p(p-1)(p-2)}{6},
\end{aligned}$$

that is the cardinalities of the sets $\mathcal{A}(p)$ and $\mathcal{B}(p)$ are equal. Since $\mathcal{A}(p) \subseteq \mathcal{B}(p)$, these sets coincide, as required. □

Corollary 2. *Consider the pairs of permutations from S_n with a 3-cycle commutator and the first permutation being a cycle of length n. Denote by $p_1(n)$ the probability that such a pair generates A_n or S_n, that is $p_1(n) = \#\mathcal{A}_1(n)/\#\mathcal{B}_1(n)$. Then the lower and the upper limits of this probability as $n \to \infty$ are equal to*

$$\liminf p_1(n) = \frac{6}{\pi^2} \qquad \textit{and} \qquad \limsup p_1(n) = 1. \tag{7}$$

Proof. Due to Corollary 1, we know that $\#\mathcal{A}_1(p)/\#\mathcal{B}_1(p) = 1$ for any prime p. Hence, $\limsup p_1(n) = 1$.
From Propositions 1 and 2 follows that

$$\frac{\#\mathcal{A}_1(n)}{\#\mathcal{B}_1(n)} = \frac{\frac{n}{6}\big(J_2(n) - 3J_1(n)\big)\,n!}{C_n^3\,n!} = \frac{J_2(n) - 3J_1(n)}{(n-1)(n-2)} \underset{n\to\infty}{\sim} \frac{J_2(n)}{n^2} - \frac{3J_1(n)}{n^2}.$$

Jordan's totient function $J_1(n) = \phi(n)$ is defined as the number of positive integers not greater than n and coprime with n. Thus, the inequality $1 \le J_1(n) \le n$ holds, from where

$$\lim_{n\to\infty} \frac{3J_1(n)}{n^2} = 0 \qquad \text{and} \qquad \liminf p_1(n) = \liminf \frac{J_2(n)}{n^2}.$$

According to the formula (A.14)

$$\frac{J_2(n)}{n^2} = \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right), \qquad \text{from where} \qquad \frac{J_2(n)}{n^2} \ge \prod_{\substack{\text{over all} \\ \text{prime } p}} \left(1 - \frac{1}{p^2}\right).$$

We conclude that

$$\liminf \frac{J_2(n)}{n^2} \ge \prod_{\substack{\text{over all} \\ \text{prime } p}} \left(1 - \frac{1}{p^2}\right).$$

Let us now show that the equality is achieved for some subsequence of the sequence $1, 2, 3, \dots$ of positive integers. Let p_k denote the k^{th} prime number ($p_1 = 2$, $p_2 = 3$, $p_3 = 5$ and so on) and take $a_k = p_1 p_2 \cdots p_k$. Then

$$\lim_{k\to\infty} \frac{J_2(a_k)}{a_k^2} = \lim_{k\to\infty} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^2}\right) = \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^2}\right).$$

The infinite product that we got here is equal to $6/\pi^2$ by the formula (A.41). Therefore,

$$\liminf p_1(n) = \liminf \frac{J_2(n)}{n^2} = \frac{6}{\pi^2},$$

as required. □

3 The case of an arbitrary cycle

Introduce the notation:

$$\mathcal{A}_2(n) = \{(s,t) \in S_n \times S_n \mid [s,t] \text{ is a 3-cycle, } s \text{ is an arbitrary cycle, } \langle s,t\rangle = A_n \text{ or } S_n\},$$

$$\mathcal{B}_2(n) = \{(s,t) \in S_n \times S_n \mid [s,t] \text{ is a 3-cycle, } s \text{ is an arbitrary cycle}\}.$$

3.1 A formula for $\#\mathcal{B}_2(n)$

Proposition 3. *The number of pairs of permutations $(s,t) \in S_n \times S_n$ with a 3-cycle commutator and s being an arbitrary cycle, is equal to*

$$\#\mathcal{B}_2(n) = \frac{1}{24}(n-1)(n-2)(n^2 + 5n + 12)\,n! \tag{8}$$

for any natural $n > 2$.

Proof. We will need Lemma 1 and the formulas (A.38) and (A.39).

Consider an arbitrary k-cycle $s \in S_n$, where $k \in [\![2, n]\!]$. A permutation $t \in S_n$ will be called **allowed for** s if

$$[s,t] = (z\ y\ x), \quad \text{that is} \quad tst^{-1} = (x\ y\ z)s. \tag{9}$$

A triple (x, y, z) of integers from the set $[\![1, n]\!]^3$ will be called **allowed for** s if the relation (9) holds for some $t \in S_n$. Herewith, we assume that the number z is *greater* than y and x. From Lemma 1 follows that a triple (x, y, z) is allowed for the permutation $s_0 = (1\ 2\ \dots\ k)$ if and only if one of the next situations occurs:

(a) The three numbers x, y, z lie in the cycle $(1\ 2\ \dots\ k)$ in the given order, that is $1 \le x < y < z \le k$ (*cf.* Figure 7). There are exactly C_k^3 such triples.

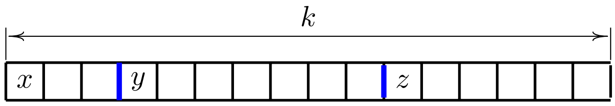

Figure 7: An allowed triple of integers $1 \le x < y < z \le k$.

(b) Two numbers x, y lie in the cycle $(1\ 2\ \dots\ k)$ and $z \in [\![k+1, n]\!]$. Moreover, $x = y + 1 \bmod k$ (*cf.* Figure 8). There are exactly $k(n-k)$ such triples, since y can be chosen in k ways and z can be chosen in $n - k$ ways.

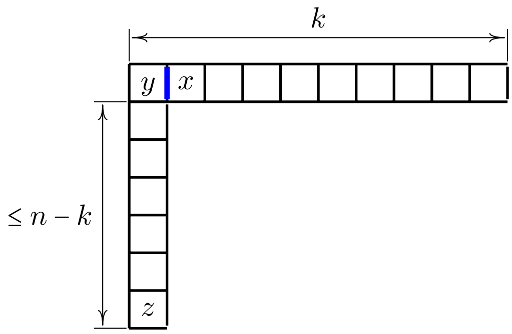

Figure 8: An allowed triple of integers $x, y \in [\![1, k]\!]$ and $z \in [\![k+1, n]\!]$, where $x = y + 1 \bmod k$.

We conclude that there are $C_k^3 + k(n-k)$ allowed triples for the k-cycle $s_0 = (1\ 2\ \dots\ k)$.

By analogy with the proof of Proposition 1, we get

$$\begin{aligned}
\#\mathcal{B}_2(n) &= \sum_{k=2}^{n} \#\{(s,t) \in S_n \times S_n \mid [s,t] = 3\text{-cycle},\ s = k\text{-cycle}\} \\
&= \sum_{k=2}^{n} \#\{s \in S_n \mid s = k\text{-cycle}\} \times \#\{t \in S_n \mid t \text{ is allowed for } s_0 = (1\ 2\ \dots\ k)\}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{k=2}^{n} \#\{s \in S_n \mid s = k\text{-cycle}\} \times |C_{S_n}(s_0)| \\
&\qquad \times \#\left\{(x,y,z) \in [\![1,n]\!]^3 \mid \text{the triple } (x,y,z) \text{ is allowed for } s_0\right\} \\
&= \sum_{k=2}^{n} n! \times \left(C_k^3 + k(n-k)\right) = \frac{n!}{6} \sum_{k=2}^{n} k(k-1)(k-2) + n! \sum_{k=2}^{n} k(n-k).
\end{aligned}$$

Finally, we apply the formula (A.39) with $r = 2$ and the formula (A.38):

$$\begin{aligned}\#\mathcal{B}_2(n) &= \frac{n!}{6}\cdot\frac{(n+1)n(n-1)(n-2)}{4} + n!\cdot\frac{(n+3)(n-1)(n-2)}{6} \\ &= \frac{n!}{24}(n-1)(n-2)\big((n+1)n + 4(n+3)\big) \\ &= \frac{1}{24}(n-1)(n-2)(n^2+5n+12)\, n!\,,\end{aligned}$$

as required. □

3.2 A formula for $\#\mathcal{A}_2(n)$

Proposition 4. *The number of pairs of permutations $(s,t) \in S_n \times S_n$ with a 3-cycle commutator, the permutation s being an arbitrary cycle and which generate A_n or S_n, is equal to*

$$\#\mathcal{A}_2(n) = \frac{n}{6}\Big(J_2(n) - 3J_1(n)\Big)\, n! + \frac{(n+1)(n-2)}{2}\, n! \tag{10}$$

for any natural $n > 2$.

Proof. We will use Proposition 2, Jordan's theorem (Proposition A.7), Lemma 1 and Proposition A.8.

From Proposition 2 we know that, in the case where s is an n-cycle, the number of required pairs is equal to

$$\#\mathcal{A}_1(n) = \frac{n}{6}\Big(J_2(n) - 3J_1(n)\Big)\, n!\,.$$

Consider now an arbitrary ℓ-cycle $s \in S_n$ with $2 \le \ell < n$. A permutation $t \in S_n$ will be called **allowed for** s if the pair (s,t) generates the group A_n or S_n and the commutator $[s,t]$ is a 3-cycle.

A triple of integers (x,y,z) from the set $[\![1,n]\!]^3$ will be called **allowed for** s if there exists an allowed permutation $t \in S_n$ for which $[s,t] = (z\ y\ x)$. Herewith, we assume that the number z is *greater* than y and x.

From Lemma 1 follows that a triple (x,y,z) is allowed for the permutation $s_0 = (1\ 2\ \ldots\ \ell)$ if and only if x and y lie in the cycle $(1\ 2\ \ldots\ \ell)$ and $z \in [\![\ell+1,n]\!]$ with condition that $x = y+1 \bmod \ell$ (*cf.* Figure 9). There are exactly $\ell(n-\ell)$ such triples, since y can be chosen in ℓ ways and z can be chosen in $n-\ell$ ways.

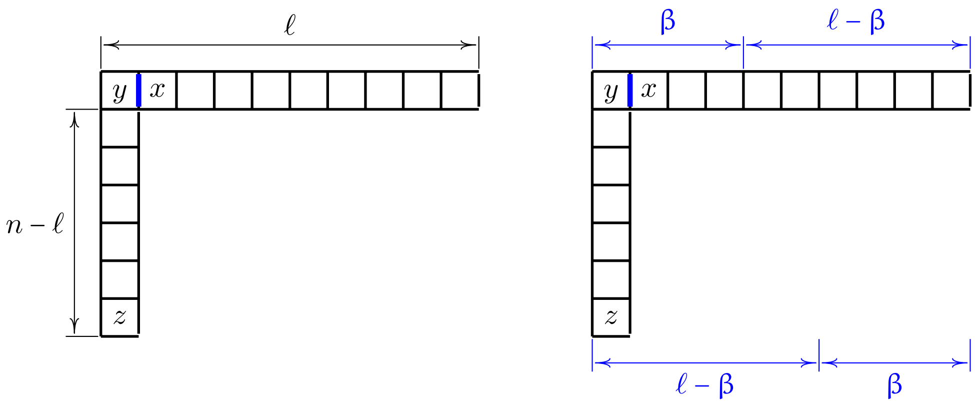

Figure 9: An allowed triple of integers $x, y \in [\![1,\ell]\!]$ and $z \in [\![\ell+1,n]\!]$, where $x = y+1 \bmod \ell$.

For a fixed ℓ-cycle $s_0 \in S_n$ and a fixed triple $(x,y,z) \in [\![1,n]\!]^3$, let us find the number of allowed permutations $t \in S_n$ such that

$$[s_0,t] = (z\ y\ x), \quad \text{that is} \quad t s_0 t^{-1} = (x\ y\ z)s_0\,. \tag{11}$$

Any such permutation t can be expressed as

$$t = (y\ z)\cdot u \cdot s_0^{\beta}, \tag{12}$$

where u is some $(n-\ell)$-cycle containing all integers from $\ell+1$ to n, and the parameter $\beta \in [\![0, \ell-1]\!]$ is a twist (*cf.* also Figure. 2). Indeed, since the group $\langle s, t\rangle$ is transitive, then the two-cylinder origami $O(s,t)$ given in Figure 9 consists of n squares, and so $t = (y\ z)\, u\, s_0^{\beta}$. Conversely: if $t = (y\ z)\, u\, s_0^{\beta}$ then the pair (s_0, t) generates the group A_n or S_n. This follows from Proposition A.8, since

$$s_0 = (y+1\ \ldots\ \ell\ 1\ \ldots\ y) \quad \text{and} \quad s_0 t s_0^{-\beta} = s_0(y\ z\ z_2\ \ldots\ z_{n-\ell}) = (y+1\ \ldots\ \ell\ 1\ \ldots\ y\ z\ z_2\ \ldots\ z_{n-\ell}),$$

where $u = (z\ z_2\ \ldots\ z_{n-\ell})$. In other words, after renumbering the points from 1 to n, we will get $s_0 = (1\,2\ \ldots\ \ell)$ and $t = (1\,2\ \ldots\ n)$.

The number of permutations t of form (12) is equal to

$$\frac{(n-\ell)!}{n-\ell}\cdot \ell,$$

since there are $\frac{1}{n-\ell}(n-\ell)!$ ways to choose an $(n-\ell)$-cycle u and ℓ ways to choose β.

We conclude that

$$\begin{aligned}
\#\mathcal{A}_2(n) &= \#\mathcal{A}_1(n) + \sum_{\ell=2}^{n-1} \#\{(s,t)\in S_n\times S_n \mid [s,t] = \text{3-cycle},\ s = \ell\text{-cycle},\ \langle s,t\rangle = A_n \text{ or } S_n\} \\
&= \#\mathcal{A}_1(n) + \sum_{\ell=2}^{n-1} \#\{s\in S_n \mid s = \ell\text{-cycle}\} \times \#\{t\in S_n \mid t \text{ is allowed for } s_0 = (1\,2\ \ldots\ \ell)\} \\
&= \#\mathcal{A}_1(n) + \sum_{\ell=2}^{n-1} \#\{s\in S_n \mid s = \ell\text{-cycle}\} \times \\
&\qquad \times \frac{(n-\ell)!}{n-\ell}\cdot \ell \times \#\left\{(x,y,z)\in [\![1,n]\!]^3 \mid \text{the triple } (x,y,z) \text{ is allowed for } s_0\right\} \\
&= \#\mathcal{A}_1(n) + \sum_{\ell=2}^{n-1} \frac{1}{\ell}\cdot\frac{n!}{(n-\ell)!} \times \frac{(n-\ell)!}{n-\ell}\cdot \ell \times \ell(n-\ell) = \#\mathcal{A}_1(n) + \sum_{\ell=2}^{n-1} \ell n! \\
&= \frac{n}{6}\Big(J_2(n) - 3J_1(n)\Big) n! + \frac{(n+1)(n-2)}{2} n!,
\end{aligned}$$

as required. □

Corollary 3. *Consider the pairs of permutations from S_n with a 3-cycle commutator and the first permutation being an arbitrary cycle. Denote by $p_2(n)$ the probability that such a pair generates A_n or S_n, that is $p_2(n) = \#\mathcal{A}_2(n)/\#\mathcal{B}_2(n)$. Then one has the following lower and upper limits as $n\to\infty$*

$$\liminf\ n\cdot p_2(n) = \frac{24}{\pi^2} \qquad \text{and} \qquad \limsup\ n\cdot p_2(n) = 4. \tag{13}$$

Proof. From Propositions 3 and 4 follows that

$$\begin{aligned}
n\cdot\frac{\#\mathcal{A}_2(n)}{\#\mathcal{B}_2(n)} &= n\cdot \frac{\frac{n}{6}\Big(J_2(n)-3J_1(n)\Big)n! + \frac{(n+1)(n-2)}{2}n!}{\frac{1}{24}(n-1)(n-2)(n^2+5n+12)\,n!} \\
&= \frac{4n^2 J_2(n) - 12n^2 J_1(n) + 12n(n+1)(n-2)}{(n-1)(n-2)(n^2+5n+12)}
\end{aligned}$$

$$\underset{n\to\infty}{\sim} \frac{4J_2(n)}{n^2} - \frac{12J_1(n)}{n^2} + \frac{12}{n}.$$

Since $\dfrac{12J_1(n)}{n^2} \to 0$ and $\dfrac{12}{n} \to 0$ as $n \to \infty$, then similarly to the proof of Corollary 2 we obtain

$$\liminf\ n \cdot p_2(n) = \liminf \frac{4J_2(n)}{n^2} = \frac{24}{\pi^2} \qquad \text{and} \qquad \limsup\ n \cdot p_2(n) = \limsup \frac{4J_2(n)}{n^2} = 4,$$

as required. □

4 The case of an arbitrary permutation

Introduce the following notation:

$$\mathcal{A}(n) = \{(s,t) \in S_n \times S_n \mid [s,t] \text{ is a 3-cycle}, \langle s,t\rangle = A_n \text{ or } S_n\},$$

$$\mathcal{B}(n) = \{(s,t) \in S_n \times S_n \mid [s,t] \text{ is a 3-cycle}\}.$$

4.1 The number of all pairs: a formula for $\#\mathcal{B}(n)$

Theorem 1. *The number of pairs of permutations from S_n with a 3-cycle commutator, is equal to*

$$\#\mathcal{B}(n) = \frac{3}{8}\left(\sum_{k=1}^{n} \sigma_3(k)P(n-k) - 2\sum_{k=1}^{n} k\sigma_1(k)P(n-k) + nP(n)\right) \cdot n! \tag{14}$$

for any natural $n > 2$.

Proof. We are going to apply Lemma 1, Ramanujan's formula (Proposition A.5) and Proposition A.6.

Denote by $\mathscr{P}(n)$ the set of partitions of a positive integer n:

$$\mathscr{P}(n) = \{(a_1,\dots,a_r) \in \mathbb{N}^r \mid r \in \mathbb{N}, \quad a_1 \le \dots \le a_r \in \mathbb{N}, \quad a_1 + \dots + a_r = n\}. \tag{15}$$

Consider an arbitrary permutation $s \in S_n$ with flag $a_1 \le \dots \le a_r$, where

$$a_1 + \dots + a_r = n \tag{16}$$

(*cf.* the section A.3 of Appendix). A permutation $t \in S_n$ will be called **allowed for** s if

$$[s,t] = (z\ y\ x), \quad \text{that is} \quad tst^{-1} = (x\ y\ z)s. \tag{17}$$

A triple (x,y,z) from the set $[\![1,n]\!]^3$ will be said to be **allowed for** s, if the relation (17) holds for some allowed $t \in S_n$. Herewith, we assume that the integer z is *greater* than y and x. According to Lemma 1, one of the two following situations occurs:

(a) All three integers x,y,z lie in the same cycle of the permutation s in the given order. There are exactly $C^3_{a_1} + \dots + C^3_{a_r}$ such triples, where $C^3_1 = C^3_2 = 0$. In this case, the triple $(x,y,z) \in [\![1,n]\!]^3$ and the permutation $t \in S_n$ with condition (17) will be called **allowed for** s **of first kind**. Let us find the number of pairs $(s,t) \in S_n \times S_n$ when t is allowed of first kind:

$$f(n) := \sum_{(a_1,\dots,a_r)\in\mathscr{P}(n)} \#\{(s,t) \in S_n \times S_n \mid \mathsf{flag}(s) = a_1,\dots,a_r,\ \ t \text{ is allowed for } s \text{ of first kind}\}$$

$$= \sum_{(a_1,\dots,a_r)\in\mathscr{P}(n)} \#\{s \in S_n \mid \mathsf{flag}(s) = a_1,\dots,a_r\}$$

$$\times \#\{t \in S_n \mid t \text{ is allowed for } s_0 \text{ of first kind}\},$$

where $s_0 = (1\ 2\ \ldots\ a_1)(a_1{+}1\ \ a_1{+}2\ \ \ldots\ \ a_1{+}a_2)\cdots(a_1{+}\cdots{+}a_{r-1}{+}1\ \ a_1{+}\cdots{+}a_{r-1}{+}2\ \ \ldots\ \ a_1{+}\cdots{+}a_r)$, and $\mathsf{flag}(s)$ denotes the flag of the permutation (*cf.* Appendix A.3).

$$\begin{aligned} f(n) &= \sum_{(a_1,\ldots,a_r)\in\mathscr{P}(n)} \#\{s\in S_n \mid \mathsf{flag}(s)=a_1,\ldots,a_r\} \times |C_{S_n}(s_0)| \\ &\qquad\qquad \times \#\left\{(x,y,z)\in[\![1,n]\!]^3 \mid \text{the triple } (x,y,z) \text{ is allowed for } s_0 \text{ of first kind}\right\} \\ &= \sum_{(a_1,\ldots,a_r)\in\mathscr{P}(n)} n! \times \left(C_{a_1}^3+\cdots+C_{a_r}^3\right) = n! \sum_{(a_1,\ldots,a_r)\in\mathscr{P}(n)} \left(C_{a_1}^3+\cdots+C_{a_r}^3\right). \end{aligned}$$

In order to simplify the last sum, we will proceed as follows. If we run over all partitions (16) of the positive integer n and count the number of ones, then we will get

$$P(n-1)+P(n-2)+\cdots+P(1)+P(0),$$

where $P(n)$ is the partition function (*cf.* the section A.2). Indeed, there are $P(n-1)$ partitions with at least one '1' (that is $a_1=1$), exactly $P(n-2)$ partitions with at least two '1's (that is $a_1=1$ and $a_2=1$), and so on, exactly $P(0)=1$ partitions with n ones. Analogically, the general statement is true: the number of parts of length d in the partitions of the integer n, is equal to

$$P(n-d)+P(n-2d)+\cdots+P(n-md), \qquad \text{where } m=\left[\frac{n}{d}\right].$$

Thus,

$$f(n) = n! \sum_{(a_1,\ldots,a_r)\in\mathscr{P}(n)} \left(C_{a_1}^3+\cdots+C_{a_r}^3\right) = n! \sum_{d=1}^{n} \left(P(n-d)+P(n-2d)+\cdots+P(n-[{}^{n}\!/d]d)\right)\cdot C_d^3 .$$

Let us regroup the summands in the last sum, by gathering the coefficients of $P(n-k)$ for $k\in[\![1,n]\!]$. For instance, the term $P(n-6)$ occurs 4 times in the sum: as a multiplier of C_1^3, C_2^3, C_3^3 and C_6^3. We obtain that

$$\begin{aligned} \frac{f(n)}{n!} &= \sum_{k=1}^{n}\left(\sum_{d|k} C_d^3\right) P(n-k) = \frac{1}{6}\sum_{k=1}^{n}\left(\sum_{d|k} d(d-1)(d-2)\right) P(n-k) \\ &= \frac{1}{6}\sum_{k=1}^{n}\left(\sum_{d|k} d^3-3d^2+2d\right) P(n-k) \\ &= \sum_{k=1}^{n}\left(\frac{1}{6}\sigma_3(k)-\frac{1}{2}\sigma_2(k)+\frac{1}{3}\sigma_1(k)\right) P(n-k), \end{aligned} \tag{18}$$

where $\sigma_i(n)$ is the sum of i^{th} powers of the divisors of n, *cf.* the formula (A.12).

(b) Two integers x and y lie in the same cycle of the permutation s, and the number z is in another cycle. Moreover, the length of the latter cycle equals the s-distance from y to x. In this case, the triple $(x,y,z)\in[\![1,n]\!]^3$ and the corresponding permutations $t\in S_n$ with condition (17) will be called **allowed for s of second kind**. It is clear that if x and y lie in a cycle of length a_j and if z lies in a cycle of length a_i with $a_i<a_j$, then such a triple (x,y,z) can be chosen in $a_i\cdot a_j$ ways. Hence, the number of all allowed triples for s of second kind is equal to

$$\sum_{\substack{1\le i<j\le r \\ a_i<a_j}} a_i a_j .$$

Let us find the number of pairs $(s,t)\in S_n\times S_n$ when t is allowed of second kind:

$$\begin{aligned} g(n) &:= \sum_{(a_1,\ldots,a_r)\in\mathscr{P}(n)} \#\{(s,t)\in S_n\times S_n \mid \mathsf{flag}(s)=a_1,\ldots,a_r,\ t \text{ is allowed for } s \text{ of second kind}\} \\ &= \sum_{(a_1,\ldots,a_r)\in\mathscr{P}(n)} \#\{s\in S_n \mid \mathsf{flag}(s)=a_1,\ldots,a_r\} \\ &\qquad\qquad \times \#\{t\in S_n \mid t \text{ is allowed for } s_0 \text{ of second kind}\}, \end{aligned}$$

where s_0 is a fixed permutation with flag $(a_1, \dots, a_r)$,

$$\begin{aligned} g(n) &= \sum_{(a_1,\dots,a_r)\in\mathscr{P}(n)} \#\{s \in S_n \mid \mathsf{flag}(s) = a_1,\dots,a_r\} \times |C_{S_n}(s_0)| \\ &\qquad \times \#\left\{(x,y,z) \in [\![1,n]\!]^3 \mid \text{the triple } (x,y,z) \text{ is allowed for } s_0 \text{ of second kind}\right\} \\ &= \sum_{(a_1,\dots,a_r)\in\mathscr{P}(n)} n! \times \left(\sum_{\substack{1\le i<j\le r \\ a_i<a_j}} a_i a_j\right) = n! \sum_{\substack{(a_1,\dots,a_r)\in\mathscr{P}(n) \\ a_i<a_j}} a_i a_j \,. \end{aligned}$$

Let us simplify the last sum. If there are exactly a parts of length $k = a_i$ and exactly b parts of length $\ell = a_j$ in a partition $(a_1, \dots, a_r)$, then gather them in the sum as $ab \cdot k\ell$. Running over all distinct partitions, such a term will occur

$$P\big(n-ak-b\ell\big) - P\big(n-(a+1)k-b\ell\big) - P\big(n-ak-(b+1)\ell\big) + P\big(n-(a+1)k-(b+1)\ell\big) \tag{19}$$

times, according to the inclusion-exclusion principle. The expression (19) counts the number of partitions of n, which contain exactly a parts of length k and exactly b parts of length ℓ. Therefore,

$$\frac{g(n)}{n!} = \sum_{\substack{a,b,k,\ell\in\mathbb{N} \\ k<\ell \\ ak+b\ell\le n}} abk\ell\Big(P\big(n-ak-b\ell\big) - P\big(n-(a+1)k-b\ell\big) - P\big(n-ak-(b+1)\ell\big) + P\big(n-(a+1)k-(b+1)\ell\big)\Big),$$

from where, gathering the coefficients of $P(n-c)$ for $c \in [\![1,n]\!]$, we obtain

$$\begin{aligned} \frac{g(n)}{n!} &= \sum_{c=1}^{n} \sum_{\substack{a,b,k,\ell\in\mathbb{N} \\ k<\ell \\ ak+b\ell=c}} \Big(abk\ell - (a-1)bk\ell - a(b-1)k\ell + (a-1)(b-1)k\ell\Big)\, P(n-c) \\ &= \sum_{c=1}^{n} \sum_{\substack{a,b,k,\ell\in\mathbb{N} \\ k<\ell \\ ak+b\ell=c}} k\ell\, P(n-c) = \sum_{c=1}^{n} \left(\sum_{\substack{a,b,k,\ell\in\mathbb{N} \\ k<\ell \\ ak+b\ell=c}} k\ell\right) P(n-c)\,. \end{aligned}$$

Now, let us evaluate the following sum

$$\sum_{\substack{a,b,k,\ell\in\mathbb{N} \\ k<\ell \\ ak+b\ell=c}} k\ell = \frac{1}{2}\left(\sum_{\substack{a,b,k,\ell\in\mathbb{N} \\ ak+b\ell=c}} k\ell - \sum_{\substack{a,b,k\in\mathbb{N} \\ (a+b)k=c}} k^2\right) \tag{20}$$

From the equality $(a+b)k = c$ follows that k divides c. Moreover, for fixed k and c, exactly $c/k - 1$ pairs of positive integers (a,b) satisfy this equality (since a can take values from 1 to $c/k - 1$). We have

$$\sum_{\substack{a,b,k\in\mathbb{N} \\ (a+b)k=c}} k^2 = \sum_{k|c} \left(\frac{c}{k} - 1\right) k^2 = c\sum_{k|c} k - \sum_{k|c} k^2 = c\,\sigma_1(c) - \sigma_2(c)\,. \tag{21}$$

Further, with notation $\alpha = ak$ and $\beta = b\ell$ one has

$$\sum_{\substack{a,b,k,\ell\in\mathbb{N} \\ ak+b\ell=c}} k\ell = \sum_{\substack{\alpha,\beta\in\mathbb{N} \\ \alpha+\beta=c}} \left(\sum_{k|\alpha} k\right)\left(\sum_{\ell|\beta} \ell\right) = \sum_{\substack{\alpha,\beta\in\mathbb{N} \\ \alpha+\beta=c}} \sigma_1(\alpha)\sigma_1(\beta)\,.$$

The last sum appears in one of Ramanujan's formula (*cf.* Proposition A.5), due to which

$$\sum_{\substack{a,b,k,\ell\in\mathbb{N} \\ ak+b\ell=c}} k\ell = \sum_{\substack{\alpha,\beta\in\mathbb{N} \\ \alpha+\beta=c}} \sigma_1(\alpha)\sigma_1(\beta) = \frac{5}{12}\sigma_3(c) + \frac{1}{12}\sigma_1(c) - \frac{1}{2}c\,\sigma_1(c)\,. \tag{22}$$

The relations (20), (21) and (22) give

$$\sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=c}} k\ell = \frac{1}{2}\left(\frac{5}{12}\sigma_3(c)+\frac{1}{12}\sigma_1(c)-\frac{1}{2}c\,\sigma_1(c)-c\,\sigma_1(c)+\sigma_2(c)\right) = \frac{5}{24}\sigma_3(c)+\frac{1}{2}\sigma_2(c)+\left(\frac{1}{24}-\frac{3c}{4}\right)\sigma_1(c) \tag{23}$$

and so

$$\frac{g(n)}{n!} = \sum_{c=1}^{n}\left(\sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=c}} k\ell\right)P(n-c) = \sum_{c=1}^{n}\left(\frac{5}{24}\sigma_3(c)+\frac{1}{2}\sigma_2(c)+\left(\frac{1}{24}-\frac{3c}{4}\right)\sigma_1(c)\right)P(n-c). \tag{24}$$

Finally, summing the formulas (18) and (24), we obtain

$$\begin{aligned}
\#\mathcal{B}(n) &= \sum_{(a_1,\ldots,a_r)\in\mathscr{P}(n)} \#\{(s,t)\in S_n\times S_n \mid \mathsf{flag}(s)=a_1,\ldots,a_r,\ \ t \text{ allowed for } s\} = f(n)+g(n)\\
&= n!\sum_{k=1}^{n}\left(\frac{1}{6}\sigma_3(k)-\frac{1}{2}\sigma_2(k)+\frac{1}{3}\sigma_1(k)+\frac{5}{24}\sigma_3(k)+\frac{1}{2}\sigma_2(k)+\left(\frac{1}{24}-\frac{3k}{4}\right)\sigma_1(k)\right)P(n-k)\\
&= n!\sum_{k=1}^{n}\left(\frac{3}{8}\sigma_3(k)-\frac{3k}{4}\sigma_1(k)+\frac{3}{8}\sigma_1(k)\right)P(n-k).
\end{aligned}$$

According to Proposition A.6, the equality $\sum_{k=1}^{n}\sigma_1(k)\,P(n-k)=nP(n)$ holds for $n\in\mathbb{N}$, from where

$$\#\mathcal{B}(n) = \frac{3}{8}n!\sum_{k=1}^{n}\Big(\sigma_3(k)-2\sigma_1(k)\Big)P(n-k) + \frac{3n}{8}P(n)n!,$$

as required. □

In order to estimate the cardinality of the set $\mathcal{B}(n)$, let us show the next lemma.

Lemma 5. *For any natural $n>1$, the following inequality holds*

$$\sigma_3(n) < n^2\sigma_1(n).$$

For any $\delta>0$, there exists a positive integer $K=K(\delta)$ such that[a]

$$\sigma_3(n) > n^{2-\delta}\sigma_1(n)$$

for all natural $n\geq K$.

[a] The notation $K=K(\delta)$ means that a number K depends only on δ.

Proof. The first inequality follows from the definition of $\sigma_3(n)$ and $\sigma_1(n)$:

$$\sigma_3(n) = \sum_{d|n} d^3 < \sum_{d|n} n^2 d = n^2\sigma_1(n).$$

Consider now the arithmetic function

$$g(n) = \frac{\sigma_3(n)}{n\sigma_1(n)}.$$

Notice that it is multiplicative as a ratio of two multiplicative functions. For a power of a prime p^α, according to the formula (A.12) we have

$$\begin{aligned} g(p^\alpha) &= \frac{\sigma_3(p^\alpha)}{p^\alpha\sigma_1(p^\alpha)} = \frac{(p^{3(\alpha+1)}-1)\big/(p^3-1)}{p^\alpha\,(p^{\alpha+1}-1)\big/(p-1)} = \frac{(p^{\alpha+1}-1)(p^{2(\alpha+1)}+p^{\alpha+1}+1)}{p^\alpha(p^{\alpha+1}-1)(p^2+p+1)} \\ &= \frac{p^{2\alpha+2}\left(1+1\big/p^{\alpha+1}+1\big/p^{2\alpha+2}\right)}{p^{\alpha+2}\left(1+1\big/p+1\big/p^2\right)} = p^\alpha\cdot\frac{1+1\big/p^{\alpha+1}+1\big/p^{2\alpha+2}}{1+1\big/p+1\big/p^2} \\ &> p^\alpha\cdot\frac{1}{1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots} = p^\alpha\cdot\frac{1}{1\big/(1-\frac{1}{p})} = p^\alpha\left(1-\frac{1}{p}\right). \end{aligned}$$

Thus, for any positive integer $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r} > 1$, the following inequality holds

$$g(n) = g(p_1^{\alpha_1})\cdots g(p_r^{\alpha_r}) > p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\cdots p_r^{\alpha_r}\left(1-\frac{1}{p_r}\right) = n\prod_{\substack{p|n\\ p\text{ prime}}}\left(1-\frac{1}{p}\right) = \phi(n),$$

$$\text{that is}\qquad \sigma_3(n) > n\phi(n)\sigma_1(n), \tag{25}$$

where $\phi(n)$ is Euler's totient function, *cf.* (A.13).

Let us show that for any $\delta > 0$, there exists a natural $K = K(\delta)$ such that

$$\phi(n) > n^{1-\delta} \tag{26}$$

for all natural $n \ge K$. Consider the function

$$f(n) = \frac{n^{1-\delta}}{\phi(n)}.$$

It is multiplicative and when $n = p^\alpha$ it takes the value

$$f(p^\alpha) = \frac{p^{\alpha(1-\delta)}}{p^\alpha\left(1-1\big/p\right)} = \frac{1}{p^{\alpha\delta}}\cdot\frac{p}{p-1},$$

which tends to zero as $p^\alpha \to +\infty$. According to Proposition A.3, we conclude that $f(n) \to 0$ as $n \to +\infty$. In particular, there exists $K \in \mathbb{N}$ such that

$$f(n) < 1 \quad \text{for all } n \ge K.$$

This proves the inequality (26), from where taking into account the inequality (25) we obtain that

$$\sigma_3(n) > n\phi(n)\sigma_1(n) > n^{2-\delta}\sigma_1(n) \quad \text{for all } n \ge K,$$

as required. □

For a real number a, consider the following arithmetic function:

$$\psi_a(n) = \sum_{k=1}^{n} k^a\sigma_1(k)P(n-k). \tag{27}$$

In Proposition A.6 it is shown that $\psi_0(n) = nP(n)$. If $a \ge b$ then for any $n \in \mathbb{N}$, the inequality $\psi_a(n) \ge \psi_b(n)$ holds. We have the following simple bounds of the function $\psi_a(n)$ when $a \ge 0$:

$$nP(n) = \sum_{k=1}^{n}\sigma_1(k)P(n-k) \le \psi_a(n) \le n^a\sum_{k=1}^{n}\sigma_1(k)P(n-k) = n^{a+1}P(n). \tag{28}$$

In particular, $nP(n) \le \psi_2(n) \le n^3P(n)$.

Let us now estimate the cardinality of the set $\mathcal{B}(n)$.

Corollary 4. *For any $\epsilon > 0$, there exists a positive integer $N = N(\epsilon)$ such that*

$$\psi_{2-\epsilon}(n) \cdot n! \; < \; \#\mathcal{B}(n) \; < \; \frac{3}{8}\psi_2(n) \cdot n!$$

for all natural $n \geq N$.

Proof. From Theorem 1, the relation $\psi_0(n) = nP(n)$, the inequality $\psi_1(n) \geq \psi_0(n)$ and the inequality $\sigma_3(k) \leq k^2\sigma(k)$ in Lemma 5 follows that

$$\begin{aligned}
\frac{8}{3} \cdot \frac{\#\mathcal{B}(n)}{n!} \; &= \; \sum_{k=1}^{n} \sigma_3(k)P(n-k) \; - \; 2\psi_1(n) \; + \; \psi_0(n) \\
&\leq \; \sum_{k=1}^{n} k^2\sigma_1(k)P(n-k) \; - \; 2\psi_0(n) \; + \; \psi_0(n) \; = \; \psi_2(n) - \psi_0(n) \\
&< \; \psi_2(n),
\end{aligned}$$

which proves the upper bound of the cardinality of $\mathcal{B}(n)$ for all $n \in \mathbb{N}$.

Let ϵ be an arbitrary positive real number. Choose any number $\delta > 0$ with conditions $\delta < 1$ and $\delta < \epsilon$. According to Lemma 5, there exists a positive integer K such that $\sigma_3(k) > k^{2-\delta}\sigma_1(k)$ for all natural $k \geq K$. Then

$$\begin{aligned}
\sum_{k=1}^{n} \sigma_3(k)P(n-k) \; &= \; \sum_{k=K}^{n} \sigma_3(k)P(n-k) + \sum_{k=1}^{K-1} \sigma_3(k)P(n-k) \\
&> \; \sum_{k=K}^{n} k^{2-\delta}\sigma_1(k)P(n-k) + \sum_{k=1}^{K-1} \sigma_3(k)P(n-k) \\
&> \; \sum_{k=K}^{n} k^{2-\delta}\sigma_1(k)P(n-k).
\end{aligned}$$

In the right side of this inequality, let us add and subtract the expression $\sum_{k=1}^{K-1} k^{2-\delta}\sigma_1(k)P(n-k)$, getting

$$\begin{aligned}
\sum_{k=1}^{n} \sigma_3(k)P(n-k) \; &> \; \sum_{k=1}^{n} k^{2-\delta}\sigma_1(k)P(n-k) \; - \; \sum_{k=1}^{K-1} k^{2-\delta}\sigma_1(k)P(n-k) \\
&> \; \psi_{2-\delta}(n) \; - \; K^5P(n),
\end{aligned} \tag{29}$$

since $k^{2-\delta} < K^2$, $\sigma_1(k) \leq k^2 < K^2$ and $P(n-k) < P(n)$ for $1 \leq k < K$.

From the conditions $\delta < 1$ and $\delta < \epsilon$ follows that

$$\frac{2k + \frac{8}{3}k^{2-\epsilon}}{k^{2-\delta}} \; = \; \frac{2}{k^{1-\delta}} + \frac{8/3}{k^{\epsilon-\delta}} \; \underset{k\to+\infty}{\longrightarrow} \; 0.$$

Hence, there is a natural $L = L(\epsilon)$ such that

$$\frac{2k + \frac{8}{3}k^{2-\epsilon}}{k^{2-\delta}} < 1, \quad \text{that is} \quad k^{2-\delta} - 2k > \frac{8}{3}k^{2-\epsilon} \quad \text{for } k \geq L.$$

When $1 \leq k < L$, one has the inequalities $k^{2-\delta} - 2k - \frac{8}{3}k^{2-\epsilon} > k - 2k - 3k^2 \geq -L - 3L^2 \geq -4L^2$, that is

$k^{2-\delta} - 2k > \frac{8}{3}k^{2-\epsilon} - 4L^2$. Therefore, we obtain

$$\begin{aligned}
\psi_{2-\delta}(n) - 2\psi_1(n) &= \sum_{k=1}^{n} \left(k^{2-\delta} - 2k\right) \cdot \sigma_1(k) P(n-k) \\
&= \sum_{k=L}^{n} \left(k^{2-\delta} - 2k\right) \cdot \sigma_1(k) P(n-k) + \sum_{k=1}^{L-1} \left(k^{2-\delta} - 2k\right) \cdot \sigma_1(k) P(n-k) \\
&> \sum_{k=L}^{n} \frac{8}{3} k^{2-\epsilon} \sigma_1(k) P(n-k) + \sum_{k=1}^{L-1} \left(\frac{8}{3} k^{2-\epsilon} - 4L^2\right) \cdot \sigma_1(k) P(n-k) \\
&> \frac{8}{3} \sum_{k=1}^{n} k^{2-\epsilon} \sigma_1(k) P(n-k) - L \cdot 4L^2 \cdot L^2 P(n) = \frac{8}{3} \psi_{2-\epsilon}(n) - 4L^5 P(n),
\end{aligned}$$

since $\sigma_1(k) \le k^2 < L^2$ and $P(n-k) < P(n)$, when $1 \le k < L$.

By applying this inequality and the inequality (29), we get the following bound

$$\begin{aligned}
\frac{8}{3} \cdot \frac{\#\mathcal{B}(n)}{n!} &= \sum_{k=1}^{n} \sigma_3(k) P(n-k) - 2\psi_1(n) + nP(n) \\
&> \psi_{2-\delta}(n) - 2\psi_1(n) - K^5 P(n) + nP(n) \\
&> \frac{8}{3} \psi_{2-\epsilon}(n) + \left(n - K^5 - 4L^5\right) \cdot P(n) \\
&> \frac{8}{3} \psi_{2-\epsilon}(n) \qquad \text{for } n \ge N,
\end{aligned}$$

where a constant $N = K^5 + 4L^5$ depends on δ and ϵ. In its turn, the choice of δ was based on the number ϵ. Therefore, N depends only on ϵ.

We conclude that for any $\epsilon > 0$, there exists a natural $N = N(\epsilon)$ such that $\#\mathcal{B}(n) > \psi_{2-\epsilon}(n) \cdot n!$ for all $n \ge N$. This completes the proof of Corollary. □

The next statement is an application of Theorem 1 to the theory of representations of the symmetric group (several main definitions are given in Appendix A.4).

Corollary 5. *Let $c \in S_n$ be any 3-cycle. For all natural $n > 2$ the following relation holds*

$$\frac{8}{9} n(n-1)(n-2) \sum_{\rho} \frac{\chi_\rho(c)}{\dim \rho} = nP(n) + \sum_{k=1}^{n} \Big(\sigma_3(k) - 2k\, \sigma_1(k)\Big) P(n-k),$$

where the sum is over all (pairwise nonequivalent) irreducible representations ρ of S_n, and χ_ρ denotes the character of ρ.

In particular, one has the bounds

$$\frac{3}{n^2} P(n) < \sum_{\rho} \frac{\chi_\rho(c)}{\dim \rho} < \frac{5}{4} P(n)$$

for any sufficiently large n.

Proof. According to Frobenius's formula for $u = c$ (*cf.* Proposition A.9), we have

$$\#\mathcal{B}(n) = n! \cdot \frac{n(n-1)(n-2)}{3} \cdot \sum_{\rho} \frac{\chi_\rho(c)}{\dim \rho}.$$

Comparing with Theorem 1, we get the required relation.

We know from Corollary 4 with $\epsilon = 2$ that, for sufficiently large n, the following inequalities hold

$$\psi_0(n) < \frac{\#\mathcal{B}(n)}{n!} < \frac{3}{8}\psi_2(n), \qquad \text{and so} \qquad nP(n) < \frac{\#\mathcal{B}(n)}{n!} < \frac{3}{8}n^3P(n),$$

since $\psi_0(n) = nP(n)$ and $\psi_2(n) \le n^3P(n)$. Therefore,

$$\frac{3}{(n-1)(n-2)}P(n) < \sum_\rho \frac{\chi_\rho(c)}{\dim\rho} < \frac{9}{8}\cdot\frac{n^2}{(n-1)(n-2)}P(n).$$

But $\frac{3}{n^2} < \frac{3}{(n-1)(n-2)}$ and for sufficiently large n one has

$$\frac{9}{8}\cdot\frac{n^2}{(n-1)(n-2)} = \frac{9}{8}\cdot\frac{1}{(1-\frac{1}{n})(1-\frac{2}{n})} < \frac{10}{8} = \frac{5}{4}.$$

This proves the required bounds. □

4.2 The number of primitive pairs: a formula for $\#\mathcal{A}(n)$

Lemma 6. *Vectors $\overrightarrow{(\alpha,a)}$, $\overrightarrow{(\beta,b)}$, $\overrightarrow{(k,0)}$ and $\overrightarrow{(\ell,0)}$ generate the lattice $\mathbb{Z}^2$ if and only if the following two conditions are stisfied:*

$$a \wedge b = 1 \qquad \textit{and} \qquad k \wedge \ell \wedge (a\beta - b\alpha) = 1.$$

Proof. ($\Longrightarrow$) The condition $a \wedge b = 1$ is necessary, since the ordinate of any linear combination with integer coefficients of the four given vectors is obviously divisible by the greatest common divisor of a and b. Suppose that the vectors $\overrightarrow{(\alpha,a)}$, $\overrightarrow{(\beta,b)}$, $\overrightarrow{(k,0)}$, $\overrightarrow{(\ell,0)}$ generate $\mathbb{Z}^2$ and that $a \wedge b = 1$. Let us find all integers p, for which the system of equations

$$\begin{cases} \alpha X + \beta Y = p, \\ aX + bY = 0 \end{cases}$$

has a solution in integers X and Y. We get $aX = -bY$, which is equivalent to equalities $X = -mb$ and $Y = ma$ for some $m \in \mathbb{Z}$, since a and b are coprime. From this we obtain

$$p = \alpha X + \beta Y = m(a\beta - b\alpha),$$

which is a multiple of $a\beta - b\alpha$.

By assumption, the vector $\overrightarrow{(1,0)}$ is a linear combination

$$X\overrightarrow{(\alpha,a)} + Y\overrightarrow{(\beta,b)} + Z\overrightarrow{(k,0)} + W\overrightarrow{(\ell,0)}$$

with integer coefficients X, Y, Z and W. This is possible only if

$$m(a\beta - b\alpha) + Zk + W\ell = 1 \quad \text{for some integers } m, Z \text{ and } W, \tag{30}$$

that is if the numbers $a\beta - b\alpha$, k and ℓ are coprime.

($\Longleftarrow$) Conversely, suppose that the conditions $a \wedge b = 1$ and $k \wedge \ell \wedge (a\beta - b\alpha) = 1$ are satisfied. From the second condition follows that the equality (30) holds, and so

$$-mb\overrightarrow{(\alpha,a)} + ma\overrightarrow{(\beta,b)} + Z\overrightarrow{(k,0)} + W\overrightarrow{(\ell,0)} = \overrightarrow{(m(a\beta - b\alpha) + Zk + W\ell,\ -mba + mab)} = \overrightarrow{(1,0)}.$$

The first condition implies the existence of integers X and Y such that $Xa + Yb = 1$, from where

$$X\overrightarrow{(\alpha,a)} + Y\overrightarrow{(\beta,b)} = \overrightarrow{(X\alpha + Y\beta,\ 1)}.$$

Since linear combinations of the vector $\overrightarrow{(1,0)}$ and $\overrightarrow{(X\alpha + Y\beta,\ 1)}$ with integer coefficients cover all $\mathbb{Z}^2$, then the given four vectors generate $\mathbb{Z}^2$. □

Lemma 7. *A two-cylinder origami with parameters* $(a, b, k, \ell, \alpha, \beta)$ *is primitive if and only if the following two conditions are satisfied:*

$$a \wedge b = 1 \qquad \text{and} \qquad k \wedge \ell \wedge (a\beta - b\alpha) = 1.$$

Proof. A two-cylinder origami with parameters $(a, b, k, \ell, \alpha, \beta)$ consists of $n = ak + b\ell$ squares. Number its squares by the integers from 1 to n. Then we will get two permutations s and t from S_n that indicate how the squares are glued in the horizontal and the vertical directions respectively. Denote by G the monodromy group origami, that is the permutation group generatd by the pair (s, t).

$\boxed{\Longrightarrow}$ Suppose that the conditions $a \wedge b = 1$ and $k \wedge \ell \wedge (a\beta - b\alpha) = 1$ are not satisfied. By Lemma 6, this means that the vectors $\overrightarrow{(\alpha, a)}$, $\overrightarrow{(\beta, b)}$, $\overrightarrow{(k, 0)}$ and $\overrightarrow{(\ell, 0)}$ generate a lattice L not coinciding with the entire $\mathbb{Z}^2$. Let us show then that the square-tiled surface is not primitive, that is the permutation group $G = \langle s, t \rangle$ has a nontrivial block $\Delta \subset [\![1, n]\!]$.

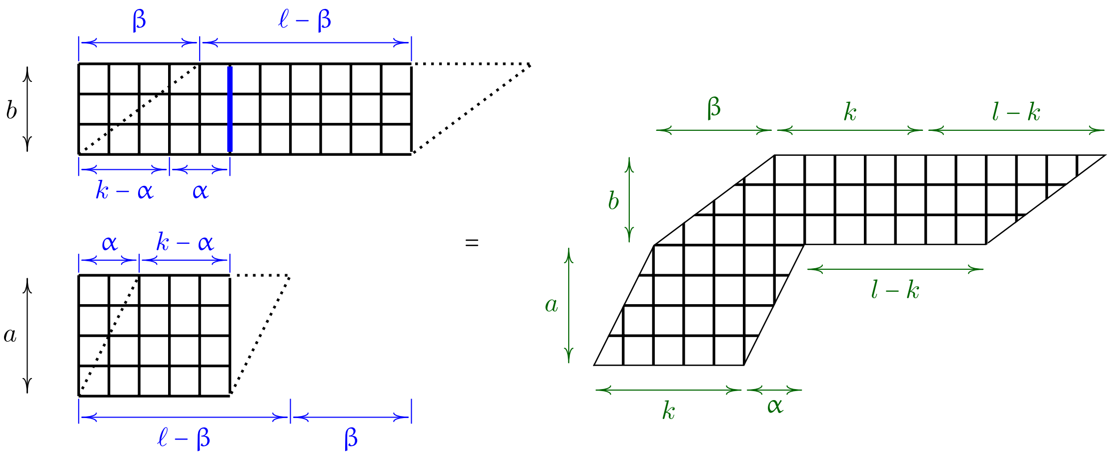

Figure 10: An unfolding of the two-cylinder square-tiled surface.

In the real plane, mark the points of the lattice L. A two-cylinder square-tiled surface can be unfolded in the plane as two glued parallelograms: the first one is constructed on the vectors $\overrightarrow{(\alpha, a)}$ and $\overrightarrow{(k, 0)}$, and the second one is constructed on the vectors $\overrightarrow{(\beta, b)}$ and $\overrightarrow{(\ell, 0)}$, see Figure 10. Place such an unfolding as shown in Figure 11. Color those squares of the surface, the lower left vertex of which is a point of the lattice L. Let us prove that the set Δ of numbers of the colored squares is a block for the group G.

Indeed, consider an arbitrary square of the surface, and let (p, q) be the coordinates of its lower left vertex. Then, when acting by the permutations s or t, this square will be sent to the square of the surface with the following coordinates of its lower left vertex:

$$(p+1, q) + \varepsilon_1 \overrightarrow{(k, 0)} + \varepsilon_2 \overrightarrow{(\ell, 0)} \qquad \text{or} \qquad (p, q+1) - \varepsilon_3 \overrightarrow{(\alpha + \beta, a + b)} - \varepsilon_4 \overrightarrow{(\beta, b)}$$

respectively, where $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 \in \{0, 1\}$. Hence, under the action of any permutation $g \in G$ (which is of course a word on the letters s and t), the coordinates of the lower left vertices of the colored squares of the surface will be translated by the same vector $\vec{v} \in \mathbb{Z}^2$ up to linear combinations of type $\varepsilon_1 \overrightarrow{(k, 0)} + \varepsilon_2 \overrightarrow{(\ell, 0)}$ and $-\varepsilon_3 \overrightarrow{(\alpha + \beta, a + b)} - \varepsilon_4 \overrightarrow{(\beta, b)}$. By definition, the lattice L consists of all linear combinations

$$m_1 \cdot \overrightarrow{(\alpha, a)} + m_2 \cdot \overrightarrow{(\beta, b)} + m_3 \cdot \overrightarrow{(k, 0)} + m_4 \cdot \overrightarrow{(\ell, 0)}.$$

Therefore, under the action of a permutation g, either the set of all marked squares will not change, or it will be sent to a set of squares not intersecting with it, that is

$$g(\Delta) = \Delta \qquad \text{or} \qquad g(\Delta) \cap \Delta = \varnothing$$

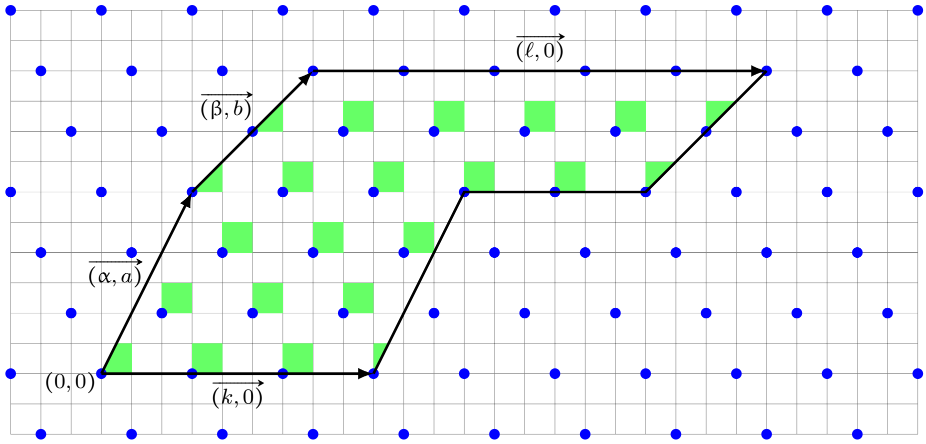

Figure 11: The marked points belong to the lattice L generated by the vectors with coordinates (α, a), (β, b), $(k, 0)$ and $(\ell, 0)$. The colored squares of the surface form a nontrivial block for the group G.

depending on whether the vector $\vec{v}$ belongs to the lattice L or not. We conclude that Δ is a block for the group G. Since the lattice L is distinct from $\mathbb{Z}^2$, the block Δ is nontrivial and the group G is not primitive.

$\Longleftarrow$ Suppose now that the conditions $a \wedge b = 1$ and $k \wedge \ell \wedge (a\beta - b\alpha) = 1$ are satisfied, and let us prove that the square-tiled surface is primitive. Unwrap the surface in the real plane as shown in Figure 12. Consider the set P of points of the plane with integer coordinates, which are situated strictly inside the unfolded surface of on its left and lower borders, excluding the points with coordinates $(k, 0)$, $(\alpha + \ell, a)$ and $(\alpha + \beta, a + b)$. This set consists of n vertices of squares of the surface. Certainly, the action of the permutation group $G = \langle s, t\rangle$ on the set $[\![1, n]\!]$, on the set of squares of the surface and on the set of points P are equivalent.

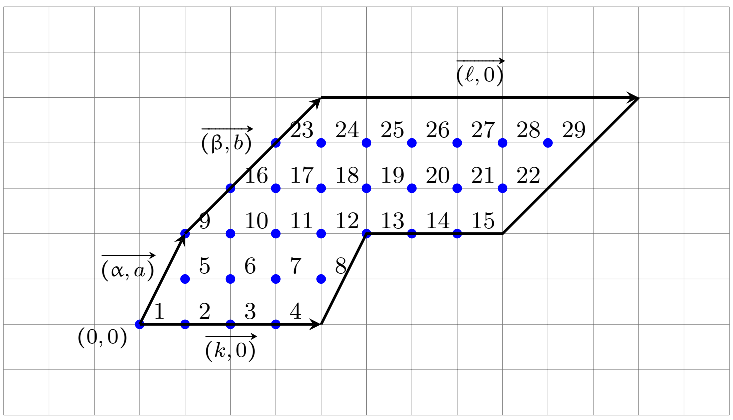

Figure 12: An unfolding of the square-tiled surface and the set P of marked points.

Let Δ_1 be an arbitrary block for G containing at least two points. Since G acts on the set P transitively (the square-tiled surface is connected), then P decomposes into several disjoint blocks of the same length:

$$P = \Delta_1 \sqcup \ldots \sqcup \Delta_m\,, \qquad \text{where } m \in \mathbb{N}\,.$$

Let us tile the plane with copies of the unfolded surface as shown in Figure 13. An infinite number of equal parallelograms, however, will stay uncovered, we will call them **teleports**. In each copy of the surface we shall mark the same integer points as in the initial one. We conclude that the following points of the plane will be marked:

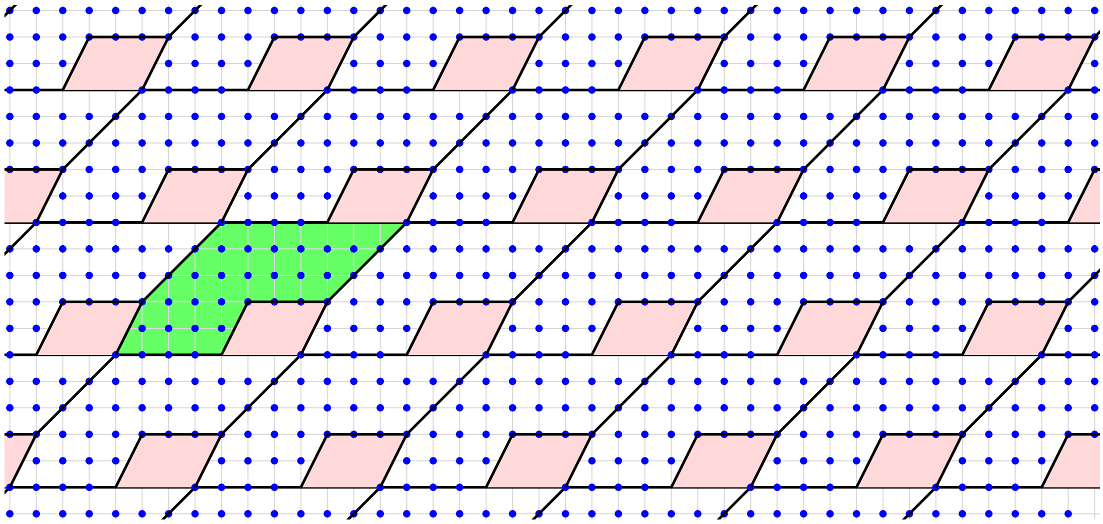

Figure 13: A tiling of the plane with copies of the unfolded square-tiled surface. An infinite number of equal parallelograms will be uncovered (teleports). The marked points form the set $\widehat{P}$.

– all integer points outside the teleports,

– all integer points on the upper and right sides of the teleports.

Consider the set $\widehat{P}$ of marked points. Denote by $\widehat{s}$ and $\widehat{t}$ the elements of the symmetric group $Sym(\widehat{P})$ which permute the points $(p,q) \in \widehat{P}$ in the following way:

$$\widehat{s}(p,q) = \begin{cases} (p+1,q), & \text{if } (p+1,q) \text{ is marked;} \\ (p+1,q)+(\ell-k,0), & \text{otherwise,} \end{cases}$$

$$\widehat{t}(p,q) = \begin{cases} (p,q+1), & \text{if } (p,q+1) \text{ is marked;} \\ (p,q+1)+(\alpha,a), & \text{if } (p,q+1) \text{ lies on the lower side of a teleport} \\ & \text{and doesn't coincides with the right end of the side,} \\ & \text{and } (p,q) \text{ is situated under the teleport;} \\ (p,q+1)-(\ell-k,0), & \text{if } (p,q+1) \text{ lies strictly inside a teleport,} \\ & \text{and } (p,q) \text{ is situated to the right of the teleport,} \\ & \text{including its right side.} \end{cases}$$

Let $\widehat{G}$ be the permutation group generatd by the pair $\widehat{s}$ and $\widehat{t}$. For all $i \in [\![1,m]\!]$, denote by $\widehat{\Delta}_i$ the subset $\widehat{P}$ consisting of the block Δ_i and all its duplicates in the copies of the unfolded surface. Then we have a decomposition of the set $\widehat{P}$ into disjoint parts:

$$\widehat{P} = \widehat{\Delta}_1 \sqcup \ldots \sqcup \widehat{\Delta}_m\,,$$

which is $\widehat{G}$-invariant, that is under the action of any permutation from $\widehat{G}$, each part $\widehat{\Delta}_i$ is sent to some $\widehat{\Delta}_j$. (It suffices to check this for the permutations $\widehat{s}$ and $\widehat{t}$, since they generate the group $\widehat{G}$.) Hence, all subsets $\widehat{\Delta}_1,\ldots,\widehat{\Delta}_m \subseteq \widehat{P}$ are blocks for the group $\widehat{G}$. We are going to show that $\widehat{\Delta}_1 = \widehat{P}$, that is $m=1$.

Connect two marked points x and y by a segment if they lie in the same block $\widehat{\Delta}_i$ for some $i \in [\![1,m]\!]$. Denote by $seg(\widehat{P})$ the set of obtained segments in the plane. To each segment xy, where $x \neq y$, corresponds two vectors $\overrightarrow{xy}$ and $\overrightarrow{yx}$ with integer coordinates, and to the segments xx corresponds the zero-vector $\overrightarrow{0}$. Let V be the set of the vectors corresponding to the segments from $seg(\widehat{P})$. The set V has the following properties:

1. *If* $\overrightarrow{xy} \in V$, *then also* $\overrightarrow{xy} \pm \overrightarrow{(\ell,0)} \in V$.

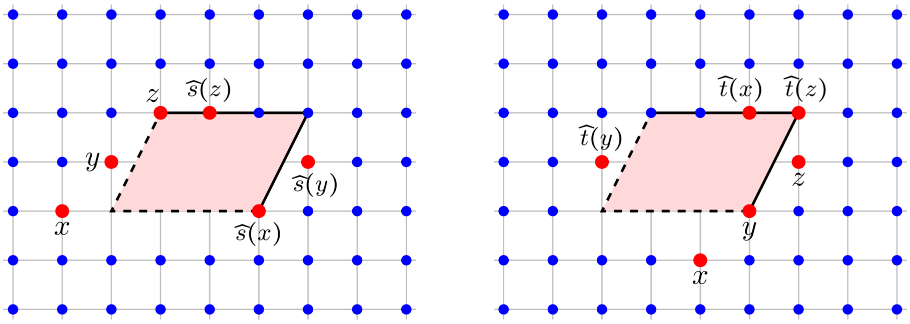

Figure 14: Actions of the permutations $\widehat{s}$ and $\widehat{t}$ on the set $\widehat{P}$.

Indeed, by construction of the blocks $\widehat{\Delta}_i$, together with each point y a block also contains the points $y \pm \overrightarrow{(\ell, 0)}$.

2. *If* $\overrightarrow{xy} \in V$, *then also* $\overrightarrow{xy} \pm \overrightarrow{(\alpha+\beta, a+b)} \in V$.

Indeed, by construction of the blocks $\widehat{\Delta}_i$, together with each point y a block also contains the points $y \pm \overrightarrow{(\alpha+\beta, a+b)}$.

3. *If* $\overrightarrow{xy} \in V$ *and the vector* $\overrightarrow{xy}$ *cannot be be presented as a linear combination*

$$c \cdot \overrightarrow{(\ell, 0)} + d \cdot \overrightarrow{(\alpha+\beta, a+b)}$$

with integer coefficients c *and* d, *then the vectors* $\overrightarrow{xy} \pm \overrightarrow{(\ell - k, 0)}$ *also belong to* V.

We can assume that the coordinates of the vector $\overrightarrow{xy} = \overrightarrow{(p, q)}$ satisfy the inequalities

$$|p| < l \quad \text{and} \quad |q| < a + b$$

in view of already proven properties 1 and 2. Besides, the vector $\overrightarrow{xy}$ is nonzero, since it is not a linear combination of the vectors $\overrightarrow{(\alpha+\beta, a+b)}$ and $\overrightarrow{(\ell, 0)}$. Let us, moreover, suppose that $p \geq 0$ and $q \geq 0$ (other cases can be treated similarly). The vector $\overrightarrow{xy}$ corresponds to a segment xy from the set $seg(\widehat{P})$. Consider the following two situations:

a) Suppose that the vector $\overrightarrow{xy}$ is not horizontal (its ordinate is nonzero). Then we can apply the permutation $\widehat{s}$ and $\widehat{t}$ to the points x and y simultaneously, so that

- the image x_1 of the point x lies on a horizontal line intersecting the interior of teleports or their lower sides;
- the image y_1 of the point y lies on a horizontal line not containing teleports or intersecting teleports by upper sides;
- moreover, $\overrightarrow{x_1y_1} = \overrightarrow{xy}$.

Such a segment x_1y_1 will belong to the set $seg(\widehat{P})$, since if x and y are in the same block $\widehat{\Delta}_i$, then the images of these points for the action of an arbitrary permutation $\widehat{w} \in \widehat{G}$ also belong to the same block, namely $\widehat{\Delta}_j = \widehat{w}(\widehat{\Delta}_i)$. Let us now apply the permutation $\widehat{s}$or $\widehat{s}^{-1}$ several times to the points x_1 and y_1, so that the point x_1 pass through the teleport situated respectively to the right or to the left of it (*cf.* Figure 15). A new segment x_2y_2 will be an element of the set $seg(\widehat{P})$, and

$$\overrightarrow{x_2y_2} = \overrightarrow{xy} - \overrightarrow{(\ell - k, 0)} \qquad \text{or} \qquad \overrightarrow{x_2y_2} = \overrightarrow{xy} + \overrightarrow{(\ell - k, 0)}$$

respectively, as required.

b) Suppose that the vector $\overrightarrow{xy}$ is horizontal. If $\overrightarrow{xy} + \overrightarrow{(\ell - k, 0)} = \vec{0}$ then we are done, since by definition $\vec{0} \in V$. Let now $\overrightarrow{xy} + \overrightarrow{(\ell - k, 0)}$ be different from $\vec{0}$. Since the vector $\overrightarrow{xy}$ is not collinear to the vector $\overrightarrow{(\alpha, a)}$, then according to the propert 4.a) below, there exists a segment $x_1y_1 \in seg(\widehat{P})$ such that

$$\overrightarrow{x_1y_1} = \overrightarrow{xy} + \overrightarrow{(\alpha, a)}\,.$$

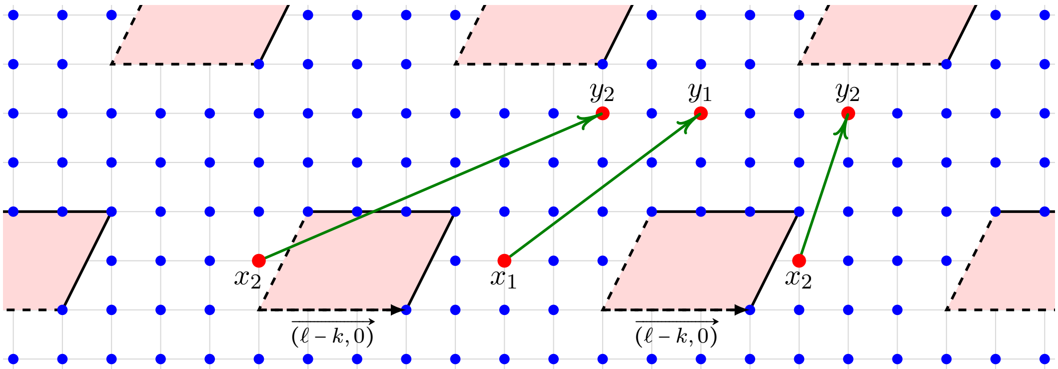

Figure 15: Vectors $\overrightarrow{x_1y_1}$ and $\overrightarrow{x_2y_2} = \overrightarrow{x_1y_1} \pm \overrightarrow{(\ell-k,0)}$ belong to the set V.

The vector $\overrightarrow{x_1y_1}$ is no more horizontal, and so by already proven property 3.a) we get a segment $x_2y_2 \in seg(\widehat{P})$, for wich

$$\overrightarrow{x_2y_2} \;=\; \overrightarrow{x_1y_1} + \overrightarrow{(\ell-k,0)} \;=\; \overrightarrow{xy} + \overrightarrow{(\ell-k,0)} + \overrightarrow{(\alpha,a)}\,.$$

The vector $\overrightarrow{xy} + \overrightarrow{(\ell-k,0)}$ is not horizontal and not equal to $\overrightarrow{0}$, from where follows that $\overrightarrow{x_2y_2}$ and $\overrightarrow{(\alpha,a)}$ are not collinear. From the property 4.a) for the vector $\overrightarrow{x_2y_2}$ follows that the vector

$$\overrightarrow{x_3y_3} \;=\; \overrightarrow{x_2y_2} - \overrightarrow{(\alpha,a)} \;=\; \overrightarrow{xy} + \overrightarrow{(\ell-k,0)}$$

also belongs to the set V.

To construct the vector $\overrightarrow{xy} - \overrightarrow{(\ell-k,0)}$, one proceeds by analogy.

4. *If $\overrightarrow{xy} \in V$ and the vector $\overrightarrow{xy}$ cannot be presented as a linear combination*

$$c \cdot \overrightarrow{(\ell,0)} + d \cdot \overrightarrow{(\alpha+\beta, a+b)}$$

with integer coefficients c and d, then the vectors $\overrightarrow{xy} \pm \overrightarrow{(\alpha,a)}$ also belong to V.

As for the property 3, we consider two situations:

a) The vector $\overrightarrow{xy}$ is not collinear to the vector $\overrightarrow{(\alpha,a)}$. One can show this by analogy with the property 3.a).

b) The vector $\overrightarrow{xy}$ is collinear to the vector $\overrightarrow{(\alpha,a)}$. A proof uses the properties 3.a) and 4.a).

Let us show now that $V = \mathbb{Z}^2$. By the initial assumption, the block Δ_1 for G contains at least two points $x, y \in P$. These points also lie in the block $\widehat{\Delta}_1$ for the group $\widehat{G}$. Hence, in the set V there is at least one vector which cannot be presented as a linear combination $c \cdot \overrightarrow{(\ell,0)} + d \cdot \overrightarrow{(\alpha+\beta, a+b)}$ with integer coefficients c and d, namely the vector $\overrightarrow{xy}$.

Let $\overrightarrow{v} \in \mathbb{Z}^2$ be an arbitrary vector with integer coordinates. According to Lemma 6, the vectors

$$\overrightarrow{(\ell,0)}, \qquad \overrightarrow{(\alpha+\beta,a+b)} = \overrightarrow{(\alpha,a)} + \overrightarrow{(\beta,b)}, \qquad \overrightarrow{(\ell-k,0)} = \overrightarrow{(\ell,0)} - \overrightarrow{(k,0)} \quad \text{and} \quad \overrightarrow{(\alpha,a)}$$

generate the lattice $\mathbb{Z}^2$. Therefore, the vector $\overrightarrow{v} - \overrightarrow{xy} \in \mathbb{Z}^2$ is of the form

$$\overrightarrow{v} - \overrightarrow{xy} \;=\; m_1 \cdot \overrightarrow{(\ell,0)} + m_2 \cdot \overrightarrow{(\alpha+\beta,a+b)} + m_3 \cdot \overrightarrow{(\ell-k,0)} + m_4 \cdot \overrightarrow{(\alpha,a)}$$

for some integers m_1, m_2, m_3 and m_4. Among all such presentations, we shall choose that, in which the sum $|m_3| + |m_4|$ is minimal. From the properties 3 and 4 follows that the vector

$$\overrightarrow{w} \;=\; \overrightarrow{xy} + m_1 \cdot \overrightarrow{(\ell,0)} + m_2 \cdot \overrightarrow{(\alpha+\beta,a+b)}$$

belongs to the set V. Since the vector $\overrightarrow{xy}$ is not a linear combination $c \cdot \overrightarrow{(\ell,0)} + d \cdot \overrightarrow{(\alpha+\beta,a+b)}$ with integer c and d, then this is also true for the vector $\overrightarrow{w}$. We may apply the property 3 for $|m_3|$ times, and after that the property 4 for $|m_4|$ times, in order to show that together with the vector $\vec{w}$ the set V also contains the vector

$$\vec{v} = \vec{w} + m_3 \cdot \overrightarrow{(\ell - k, 0)} + m_4 \cdot \overrightarrow{(\alpha, a)}.$$

Indeed, in view of the minimality of the expression $|m_3| + |m_4|$, each of the $|m_3| + |m_4| - 1$ times that we will apply the properties 3 and 4, only those vectors will occur which are not linear combinations $c \cdot \overrightarrow{(\ell, 0)} + d \cdot \overrightarrow{(\alpha + \beta, a + b)}$ for any integers c and d.

We conclude that the set V contains all vector with integer coordinates, and in particular, the vectors $\overrightarrow{(1,0)}$ and $\overrightarrow{(0,1)}$. This means that any two adjacent (vertically or horizontally) marked points lie in the same block, that is *all* marked points lie in the same block: $\widehat{\Delta}_1 = \widehat{P}$. Hence, the block Δ_1 for G is trivial (coincides with the set P), from where follows the primitivity of the group G. ☐

Lemma 8. *Let a, b, k, ℓ be positive integers with a and b being coprime. The number of distinct pairs (α, β) of integers such that*

$$0 \le \alpha < k, \quad 0 \le \beta < \ell \qquad \textit{and} \qquad k \wedge \ell \wedge (a\beta - b\alpha) = 1, \tag{31}$$

is equal to $k\ell \frac{\phi(k \wedge \ell)}{k \wedge \ell}$.

Proof. Let $k = k'd$ and $\ell = \ell' d$, where $d = k \wedge l$ is the greatest common divisor. Denote by $f(k, l)$ the number of pairs (α, β) of integers satisfying the conditions (31). Notice that if for some $\alpha', \beta' \in \mathbb{Z}$ the differences $\alpha - \alpha'$ and $\beta - \beta'$ are divisible by d, then

$$d \wedge (a\beta - b\alpha) = d \wedge \Big(a(\beta - \beta') - b(\alpha - \alpha') + a\beta' - b\alpha'\Big) = d \wedge (a\beta' - b\alpha') = 1.$$

Thus, in order to count the number of integer points (α, β) in the semi-open rectangle $[0, k[\times [0, \ell[$

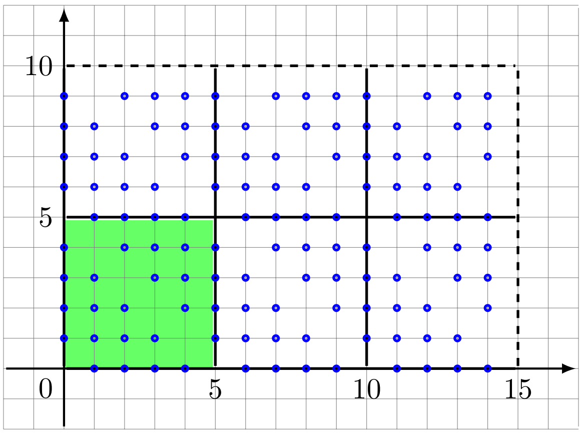

Figure 16: Integer points $(\alpha, \beta) \in [0, 15[\times [0, 10[$ such that $15 \wedge 10 \wedge (3\beta - 2\alpha) = 1$.

with condition $d \wedge (a\beta - b\alpha)$, it suffices to found the number of such points in the square $[0, d[\times [0, d[$. More precisely, by proving the equality $f(d, d) = d \cdot \phi(d)$, we will get the required:

$$f(k, l) = k'\ell' f(d, d) = k'\ell' d\phi(d) = (k'd)(\ell' d)\frac{\phi(d)}{d} = k\ell \frac{\phi(k \wedge \ell)}{k \wedge \ell}.$$

See an example in Figure 16 for $a = 3$, $b = 2$, $k = 15$, $\ell = 10$, $d = 5$.

So, let us show that the number of pairs $(\alpha, \beta) \in \mathbb{Z}^2$ with conditions

$$0 \le \alpha < d, \quad 0 \le \beta < d \qquad \text{and} \qquad d \wedge (a\beta - b\alpha) = 1$$

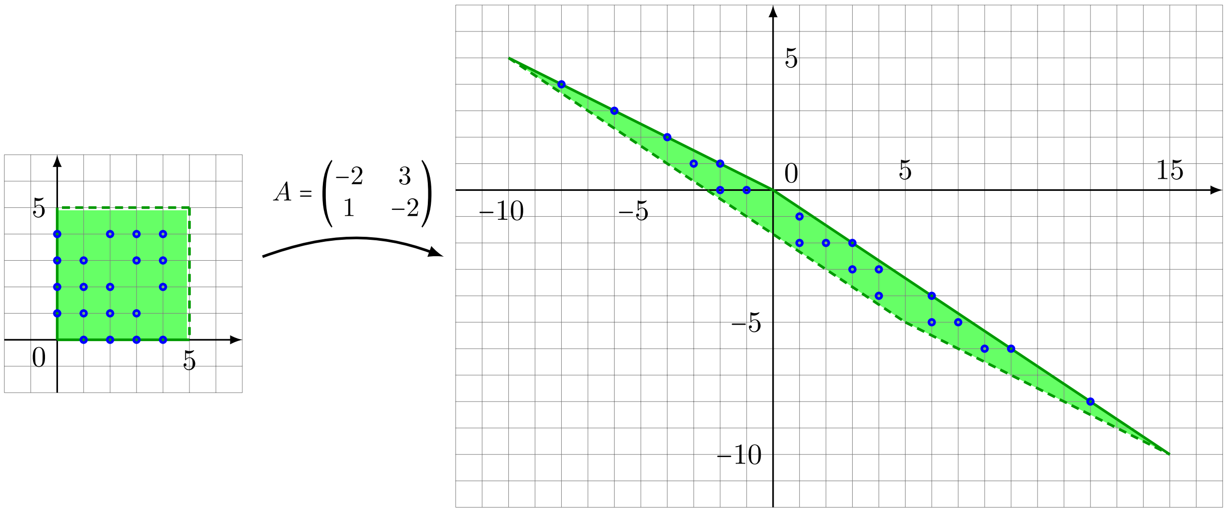

Figure 17: Integer 5-prime points in the parallelogram $A([0,5[\times[0,5[)$.

is equal to $d\phi(d)$ for any natural d. The fact that a and b are coprime guarantees the existence of integers a' and b' such that $a'a - b'b = 1$, that is the determinant of the integer matrix

$$A = \begin{pmatrix} -b & a \\ -a' & b' \end{pmatrix}$$

equals 1. An integer point (x, y) will be called **d-prime** if its first coordinate x is coprime with d. We want to find the number of integer points (α, β) in the semi-open square $K = [0, d[\times[0, d[$, for which the image

$$A \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a\beta - b\alpha \\ b'\beta - a'\alpha \end{pmatrix}$$

is a d-prime point: $d \wedge (a\beta - b\alpha) = 1$. In other words, we are interested in the number of d-prime points in the parallelogram $A(K)$, *cf.* Figure 17. Remark at once that the number of d-prime integer points (x, y) in the square K is obviously equal to $\phi(d) \cdot d$, since the first coordinate $x \in [0, d[$ can take $\phi(d)$ values for each of the d values of the second coordinate $y \in [0, d[$.

Let us show now that under the action of any integer matrix[2] $A \in SL_2(\mathbb{Z})$ on K, the number of d-prime integer points doesn't change. This is true for the matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ as shown in Figure 18. Indeed, the parallelograms $T(K)$ and $U(K)$ are obtained from the square K via translation of one of its parts by the vector $(d, 0)$ and $(0, d)$ respectively, the coordinates of which are divisible by d (this does not change the number of d-prime integer points).

Recall that the group $SL_2(\mathbb{Z})$ is generated by the pair of element T and U, that is the matrix A is a word in the alphabet $\{T, U\}$:

$$A = T^{\varepsilon_1} U^{\varepsilon_2} \dots T^{\varepsilon_{m-1}} U^{\varepsilon_m}, \qquad \text{where } \varepsilon_i \in [\![-1, 1]\!].$$

Hence, the set of integer points in the semi-open parallelogram $A(K)$ consists of integer points in the square K, that are translated by vectors with coordinates divisible by d. We conclude that in the parallelogram $A(K)$ and in the square K, there is the same number of d-prime points, namely $d \cdot \phi(d)$. This completes the proof of the equality $f(d, d) = d \cdot \phi(d)$, from where follows the required equality $f(k, l) = k\ell \frac{\phi(k\wedge\ell)}{k\wedge\ell}$. □

[2] One denotes by $SL_2(\mathbb{Z})$ the special linear group over $\mathbb{Z}$, that is the group of integer matrices 2×2 with determinant 1.

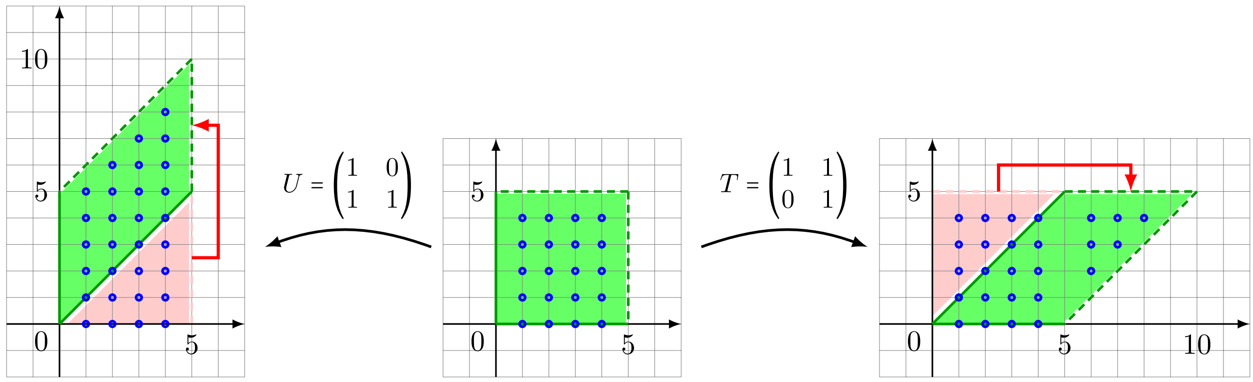

Figure 18: The number of d-prime points in the parallelograms $T(K)$ and $U(K)$ and in the square K is the same.

Theorem 2. *The number of pairs of permutations from S_n with a 3-cycle commutator and which generate A_n or S_n, is equal to*

$$\#\mathcal{A}(n) = \frac{3}{8}(n-2)J_2(n)\,n! \tag{32}$$

for any natural $n > 2$.

Proof. We are going to use Jordan's theorem (Proposition A.7), Lemma 1, Lemma 2, Proposition 2, Lemma 7, Lemma 8, the Möbius inversion formula (Proposition A.1), Dirichlet convolutions, Proposition A.4 and Ramanujan's formula (Proposition A.5).

Consider the pair of permutations $(s,t) \in S_n \times S_n$ generating the symmetric or the alternating group of degree n with condition that the commutator $[s,t]$ is a 3-cycle:

$$[s,t] = (z\ y\ x), \quad \text{that is} \quad tst^{-1} = (x\ y\ z)s. \tag{33}$$

Such a permutation $t \in S_n$ and such a triple $(x,y,z) \in [\![1,n]\!]^3$ will be called **allowed for** s. We shall always assume that $z = \max\{x,y,z\}$. Since the group $G = \langle s,t\rangle$ contains a 3-cycle, then by Jordan's theorem this group coincides with S_n or A_n if and only if it is primitive, that is *the square-tiled surface $O(s,t)$ is primitive.*

According to Lemma 1, one of the following two situations occurs:

(a) All three integers x,y,z lie in same cycle s and the square-tiled surface $O(s,t)$ is one-cylinder with some parameters (k,a,b,c), as shown in Figure 1. By Lemma 2, the surface $O(s,t)$ is primitive if and only if $k=1$ and $a \wedge b \wedge c = 1$. In particular, then the permutation s is a cycle of maximal length, and so we find the number of required pairs (s,t) via Proposition 2:

$$F(n) \ := \ \frac{n}{6}\Big(J_2(n) - 3J_1(n)\Big)\,n!\,. \tag{34}$$

(b) Two integers x and y lie in the same cycle of the permutation s, and z lies in another cycle. Moreover, the length of the latter cycle is equal to the s-distance from y to x. In this case, the square-tiled surface $O(s,t)$ is two-cylinder with parameters $(a,b,k,\ell,\alpha,\beta)$, as shown in Figure 19. According to Lemma 7, the surface $O(s,t)$ is primitive if and only if

$$a \wedge b = 1 \quad \text{and} \quad k \wedge \ell \wedge (a\beta - b\alpha) = 1.$$

Such a permutation $t \in S_n$ and such a triple $(x,y,z) \in [\![1,n]\!]^3$ will be called **allowed for** s **of second kind**. Let us find the number of pairs $(s,t) \in S_n \times S_n$, where s decomposes into a disjoint product of a cycles of length k and b cycles of length ℓ, and the permutation t is allowed

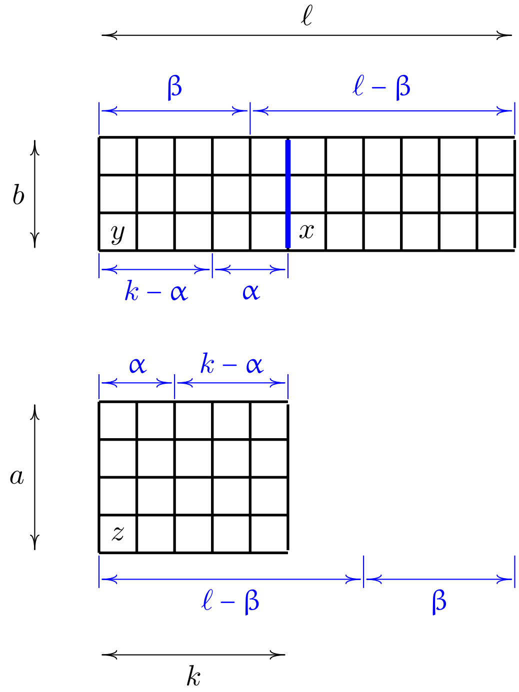

Figure 19: A two-cylinder square-tiled surface with parameters $(a, b, k, \ell, \alpha, \beta)$.

for s of second kind:

$$G(n) := \sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n\\ a\wedge b=1}} \#\left\{(s,t)\in S_n\times S_n \;\middle|\; \mathsf{type}(s)=k^a\ell^b,\ t \text{ is allowed for } s \text{ of second kind}\right\}$$

$$= \sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n\\ a\wedge b=1}} \#\left\{s\in S_n \;\middle|\; \mathsf{type}(s)=k^a\ell^b\right\} \times \#\left\{t\in S_n \;\middle|\; t \text{ is allowed for } s_0 \text{ of second kind}\right\},$$

where s_0 is a fixed permutation of cycle type $k^a\ell^b$. If a triple (x, y, z) is also fixed, then the number of allowed t for s_0 of second kind with condition (33) is equal to

$$(a-1)!\,(b-1)!\,k^a\ell^b\,\frac{\phi(d)}{d}, \qquad \text{where } d = k\wedge\ell\,.$$

Indeed, the square-tiled surface $O(s_0, t)$ in Figure 19 consists of a rows of length k and b rows of length ℓ, which correspond to the cycles of s_0. The permutation t indicates how these rows are glued:

- the row with the number z must by at the bottom, and z is in its left corner;
- the remaining $a-1$ rows of length k are glued from above in an arbitrary order, whilst a cyclic permutation of the numbers is permitted in any row – this makes $(a-1)!\,k^{a-1}$ variants;
- on top of an obtained rectangle the row with the numbers y and x is glued as shown in Figure, and a twist of length α is applied;
- the remaining $b-1$ rows of length ℓ are glued from above in an arbitrary order, whilst a cyclic permutation of the numbers is permitted in any row – this makes $(b-1)!\,\ell^{b-1}$ variants;
- finally, the top of the construction is glued to the bottom via a twist of length β.

The obtained surface must be primitive. Then by Lemma 8, there are $k\ell\,\frac{\phi(d)}{d}$ choices for the twists α and β, where $d = k\wedge\ell$. Hence, the permutation t can be chosen in $(a-1)!\,(b-1)!\,k^a\ell^b\,\frac{\phi(d)}{d}$

ways. So,

$$G(n) = \sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n\\ a\wedge b=1}} \#\left\{s\in S_n \;\middle|\; \mathsf{type}(s)=k^a\ell^b\right\} \times (a-1)!\,(b-1)!\,k^a\ell^b\,\frac{\phi(k\wedge l)}{k\wedge l}$$
$$\times\,\#\left\{(x,y,z)\in[\![1,n]\!]^3 \;\middle|\; \text{the triple } (x,y,z) \text{ is allowed for } s_0 \text{ of second kind}\right\}$$

It is easy to check that the group S_n has

$$\frac{n!}{a!\,b!\,k^a\ell^b}$$

permutations of cycle type $k^a\ell^b$. Finally, the number of allowed triples (x,y,z) of second kind for a fixed permutation s_0 of cycle type $k^a\ell^b$ is equal to

$$abk\ell\,.$$

Indeed, the integer z belongs to one of the a cycles of length k (there are $a\cdot k$ variants) and the integer y belongs to one of the b cycles of length ℓ (there are $b\cdot\ell$ variants). Therefore, we obtain the relation

$$\begin{aligned} G(n) &= \sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n\\ a\wedge b=1}} \frac{n!}{a!\,b!\,k^a\ell^b} \times (a-1)!\,(b-1)!\,k^a\ell^b\,\frac{\phi(k\wedge l)}{k\wedge l} \times abk\ell \\ &= n!\sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n\\ a\wedge b=1}} \frac{\phi(k\wedge l)}{k\wedge l} \times k\ell\,. \end{aligned}$$

Denote $g(n) = {}^{G(n)}\!/_{n!}$ and consider the following function

$$\widetilde{g}(n) := \sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n}} \frac{\phi(k\wedge l)}{k\wedge l} \times k\ell\,,$$

where integers a,b are not necessarily coprime. Denote $c=a\wedge b$ and notice that the equality $ak+b\ell=n$ is equivalent to the equality $a'k+b'\ell = {}^{n}\!/_{c}$, where the integers $a'={}^{a}\!/_{c}$ and $b'={}^{b}\!/_{c}$ are coprime. Thus,

$$\widetilde{g}(n) = \sum_{c\mid n} g(n/c) = \sum_{c\mid n} g(c)\,,$$

and by the Möbius inversion formula (Proposition A.1), we get

$$g(n) = \sum_{c\mid n}\mu(c)\widetilde{g}(n/c), \qquad \text{that is} \qquad g=\mu*\widetilde{g}\,. \tag{35}$$

Further, the greatest common divisor $d=k\wedge l$ also divides the integer $n=ak+b\ell$, from where

$$\widetilde{g}(n) = \sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n}} \frac{\phi(k\wedge l)}{k\wedge l}\,k\ell = \sum_{d\mid n}\frac{\phi(d)}{d}\left(\sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n\\ k\wedge l=d}} k\ell\right).$$

In the last sum, let us replace the pair (k,ℓ) by the pair $(d\cdot k', d\cdot \ell')$, where the integers k' and ℓ' are coprime

$$\widetilde{g}(n) = \sum_{d|n} \frac{\phi(d)}{d}\Bigg(\sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n\\ k\wedge l=d}} k\ell\Bigg) = \sum_{d|n} \frac{\phi(d)}{d}\Bigg(\sum_{\substack{a,b,k',\ell'\in\mathbb{N}\\ k'<\ell'\\ ak'+b\ell'=n\\ k'\wedge l'=1}} d^2k'\ell'\Bigg) = \sum_{d|n} d\phi(d)\Bigg(\sum_{\substack{a,b,k',\ell'\in\mathbb{N}\\ k'<\ell'\\ ak'+b\ell'={}^{n}/_{d}\\ k'\wedge l'=1}} k'\ell'\Bigg),$$

or in terms of the Dirichlet convolution:

$$\widetilde{g} = (\mathrm{id}\cdot\phi) * h, \quad \text{where} \quad h(n) = \sum_{\substack{a,b,k',\ell'\in\mathbb{N}\\ k'<\ell'\\ ak'+b\ell'=n\\ k'\wedge l'=1}} k'\ell'. \tag{36}$$

Consider also the function

$$\widetilde{h}(n) = \sum_{\substack{a,b,k,\ell\in\mathbb{N}\\ k<\ell\\ ak+b\ell=n}} k\ell.$$

Since the equality $ak+b\ell=n$ is equivalent to the equality $ak'+b\ell' = {}^{n}\!/_{d}$ with $k\ell = d^2k'\ell'$, then

$$\widetilde{h}(n) = \sum_{d|n} d^2 h(n/d), \quad \text{that is} \quad \widetilde{h} = \mathrm{id}_2 * h.$$

Taking into account Proposition A.4, we have

$$\widetilde{h} = \mathrm{id}_2\cdot\Big(\mathbb{1} * \frac{h}{\mathrm{id}_2}\Big), \quad \text{that is} \quad \frac{\widetilde{h}}{\mathrm{id}_2} = \mathbb{1} * \frac{h}{\mathrm{id}_2},$$

and so by the Möbius inversion formula, we get

$$\frac{h}{\mathrm{id}_2} = \mu * \frac{\widetilde{h}}{\mathrm{id}_2}, \quad \text{from where} \quad h = (\mathrm{id}_2\cdot\mu) * \widetilde{h}. \tag{37}$$

We conclude that the relations (35), (36) and (37) give

$$g = \mu * \widetilde{g} = \mu * (\mathrm{id}\cdot\phi) * h = \mu * (\mathrm{id}\cdot\phi) * (\mathrm{id}_2\cdot\mu) * \widetilde{h}.$$

By Proposition A.4 and the equality (A.27), one has

$$(\mathrm{id}\cdot\phi) * (\mathrm{id}_2\cdot\mu) = \mathrm{id}\cdot\big(\phi * (\mathrm{id}\cdot\mu)\big) \qquad \text{and} \qquad \phi * (\mathrm{id}\cdot\mu) = \mu,$$

from where

$$g = \mu * (\mathrm{id}\cdot\mu) * \widetilde{h}. \tag{38}$$

We already know from the proof of Theorem 1 that

$$\widetilde{h} = \frac{5}{24}\sigma_3 + \frac{1}{2}\sigma_2 + \frac{1}{24}\sigma_1 - \frac{3}{4}\mathrm{id}\cdot\sigma_1, \tag{39}$$

due to the relation (23). The equalities $\mu * \sigma_i = \mathrm{id}_i$ and $\mu * \mathrm{id}_i = J_i$ (see (A.24) and (A.23) in Appendix) imply that

$$(\mathrm{id}\cdot\mu) * \mu * \sigma_i = (\mathrm{id}\cdot\mu) * \mathrm{id}_i = \mathrm{id}\cdot(\mu * \mathrm{id}_{i-1}) = \begin{cases} \mathrm{id}\cdot(\mu * \mathbb{1}) = \mathrm{id}\cdot\varepsilon = \varepsilon, & \text{if } i=1;\\ \mathrm{id}\cdot J_{i-1}, & \text{if } i>1,\end{cases}$$

where, by definition, $\varepsilon(n) = 0$ for $n>1$. Further,

$$\mu * (\mathrm{id}\cdot\mu) * (\mathrm{id}\cdot\sigma_1) = \mu * \mathrm{id}\cdot(\mu * \sigma_1) = \mu * \mathrm{id}\cdot\mathrm{id} = \mu * \mathrm{id}_2 = J_2.$$

Put the formula (39) for $\widetilde{h}$ into the relation (38):

$$g = \frac{5}{24}\mathrm{id}\cdot J_2 + \frac{1}{2}\mathrm{id}\cdot J_1 + \frac{1}{24}\varepsilon - \frac{3}{4}J_2\,,$$

that is

$$G(n) \;=\; g(n)\,n! \;=\; \left(\frac{5}{24}nJ_2(n) + \frac{1}{2}nJ_1(n) - \frac{3}{4}J_2(n)\right)n!\,, \tag{40}$$

for any natural $n > 2$.

By summing the formulas (34) and (40), we obtain

$$\#\mathcal{A}(n) \;=\; F(n)+G(n) = \left(\frac{n}{6}J_2(n) - \frac{n}{2}J_1(n) + \frac{5n}{24}J_2(n) + \frac{n}{2}J_1(n) - \frac{3}{4}J_2(n)\right)n! \;=\; \frac{3}{8}(n-2)J_2(n)\,n!\,,$$

as required. □

Corollary 6. *For any $\epsilon > 0$, there exists a positive integer $N = N(\epsilon)$ such that*

$$n^{3-\epsilon}\cdot n! \;<\; \#\mathcal{A}(n) \;<\; \frac{3}{8}n^3\cdot n!$$

for all natural $n \geq N$.

Proof. From Theorem 2 and the definition of Jordan's totient function follows that

$$\frac{8}{3}\cdot\frac{\#\mathcal{A}(n)}{n!} \;=\; (n-2)J_2(n) \;<\; n\cdot n^2 \;=\; n^3$$

for all natural n. Let us now prove the lower bound for the cardinality of the set $\mathcal{A}(n)$. For any $\delta > 0$, there exists a number $K = K(\delta)$ such that

$$n^{2-\delta} < J_2(n) \qquad \text{for } n \geq K. \tag{41}$$

Indeed, the function

$$f(n) = \frac{n^{2-\delta}}{J_2(n)}$$

is multiplicative. For a power of a prime p^α, its value

$$f(p^\alpha) \;=\; \frac{(p^\alpha)^{2-\delta}}{(p^\alpha)^2\left(1 - {}^1\!/_{p^2}\right)} \;=\; \frac{1}{p^{\alpha\delta}}\cdot\frac{p^2}{p^2-1}$$

tends to zero as $p^\alpha \to +\infty$. According to Proposition A.3, we have $f(n) \to 0$ as $n \to +\infty$. In particular, there exists a number K such that

$$f(n) < 1 \quad \text{for all } n \geq K.$$

We conclude that if $n \geq K$ and $n \geq 4$, then

$$\frac{\#\mathcal{A}(n)}{n!} \;=\; \frac{3}{8}(n-2)J_2(n) \;>\; \frac{3}{8}\cdot\frac{n}{2}\cdot n^{2-\delta} \;=\; \frac{3}{16}n^{3-\delta}.$$

For an arbitrary $\epsilon > 0$, take $\delta = \epsilon/2$. Then

$$\begin{aligned}\frac{\#\mathcal{A}(n)}{n!} \;&>\; \frac{3}{16}n^{3-\delta} \;=\; \frac{3}{16}n^{3-\epsilon+\epsilon/2} \;=\; \frac{3n^{\epsilon/2}}{16}\cdot n^{3-\epsilon}\\ &>\; n^{3-\epsilon} \qquad \text{for } \; n \geq N,\end{aligned}$$

where $N = N(\epsilon)$ is a positive integer such that $N \geq K$, $N \geq 4$ and $N^{\epsilon/2} > {}^{16}\!/_3$. This completes the proof. □

Corollary 7. *The probability that a pair of permutations from S_n with a 3-cycle commutator generates A_n or S_n, tends to zero as $n \to +\infty$.*

Proof. According to Corollary 6, the upper bound $\#\mathcal{A}(n) < \frac{3}{8}n^3 \cdot n!$ holds for any n. On the other hand, due to Corollary 4 with $\epsilon = 2$, there exists an N such that

$$\#\mathcal{B}(n) > \psi_0(n) \cdot n! = n\,P(n) \cdot n!$$

for all $n \geq N$. Therefore,

$$0 < \frac{\#\mathcal{A}(n)}{\#\mathcal{B}(n)} < \frac{\frac{3}{8}n^2}{P(n)} \underset{n\to+\infty}{\longrightarrow} 0, \qquad \text{from where} \quad \frac{\#\mathcal{A}(n)}{\#\mathcal{B}(n)} \underset{n\to+\infty}{\longrightarrow} 0,$$

which proves the required statement. □

Appendix A Background in number theory and permutation groups

A.1 Arithmetic functions

The majority of facts about arithmetic functions, which are given in this section, can be found in the classical textbook by Apostol [1].

Definition. Any function $f : \mathbb{N} \to \mathbb{C}$ defined on the set of positive integers and taking its values in the set of complex numbers is called **arithmetic**.

Denote by $\mathcal{F}$ the set of all arithmetic functions, and by $\mathcal{F}^*$ the subset functions different from zero at the point 1:

$$\mathcal{F}^* = \{ f \in \mathcal{F} \mid f(1) \neq 0 \}. \tag{A.1}$$

For any two arithmetic functions f and g one defines their **product** $f \cdot g$:

$$(f \cdot g)(n) = f(n)g(n), \tag{A.2}$$

their **discrete convolution** $f \vartriangle g$:

$$(f \vartriangle g)(1) = 0 \quad \text{and} \quad (f \vartriangle g)(n) = \sum_{k=1}^{n-1} f(k)g(n-k) \quad \text{for } n > 1, \tag{A.3}$$

and also the **Dirichlet convolution** $f * g$:

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d). \tag{A.4}$$

The latter operation provides the structure of an abelian group on the set $\mathcal{F}^*$, since it possesses the following properties:

(*identity element*) $f * \varepsilon = \varepsilon * f = f$ for any function $f \in \mathcal{F}$, where

$$\varepsilon(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases} \tag{A.5}$$

(*inverse element*) for any $f \in \mathcal{F}^*$ there exists a unique function $\widetilde{f} \in \mathcal{F}^*$ such that $f * \widetilde{f} = \widetilde{f} * f = \varepsilon$, such a function satisfies the recurrent relation

$$\widetilde{f}(1) = \frac{1}{f(1)} \quad \text{and} \quad \widetilde{f}(n) = \frac{-1}{f(1)} \sum_{d|n,\, d<n} \widetilde{f}(d) f(n/d) \quad \text{for } n > 1; \tag{A.6}$$

(*associativity*) $f * (g * h) = (f * g) * h$ for any $f, g, h \in \mathcal{F}$;

(*commutativity*) $f * g = g * f$ for any $f, g \in \mathcal{F}$.

Definition. An arithmetic function f is **multiplicative**, if $f(1) = 1$ and the equality

$$f(mn) = f(m)f(n) \quad \text{holds for any coprime } m, n \in \mathbb{N}. \tag{A.7}$$

By $\mathcal{F}_{\text{mult}}$ we denote the set of all multiplicative arithmetic functions. It is a subgroup of the group $\mathcal{F}^*$, since

(*multiplicativity of the convolution*) the Dirichlet convolution of two multiplicative functions is multiplicative;

$\left(\begin{matrix}\textit{multiplicativity}\\ \textit{of the inverse element}\end{matrix}\right)$ the function $\widetilde{f}$ is multiplicative for any function $f \in \mathcal{F}_{\text{mult}}$.

It is easy to show that the following arithmetic functions are multiplicative:

$\mathbb{1}(n)$ **constant function**, $\mathbb{1}(n) = 1$

$\text{id}(n)$ **identical function**, $\text{id}(n) = n$

$\text{id}_k(n)$ **power function of order** k,

$$\text{id}_k(n) = n^k, \tag{A.8}$$

in particular, $\text{id}_0 = \mathbb{1}$ and $\text{id}_1 = \text{id}$

$\mu(n)$ **Möbius function** defined as

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^r, & \text{if } \alpha_1 = \ldots = \alpha_r = 1 \\ 0, & \end{cases} \tag{A.9}$$

where $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factorization of n

$\tau(n)$ **number of divisors** of n,

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1), \tag{A.10}$$

where $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factorization of n

$\sigma(n)$ **sum of divisors** of n,

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}, \tag{A.11}$$

where $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factorization of n

$\sigma_k(n)$ **sigma-function of order** k is the sum of k^{th} powers of the divisors of n,

$$\sigma_k(n) = \sum_{d|n} d^k = \prod_{i=1}^{r} \frac{p_i^{k(\alpha_i+1)} - 1}{p_i^k - 1}, \tag{A.12}$$

in particular, $\sigma_0 = \tau$ and $\sigma_1 = \sigma$

$\phi(n)$ **Euler's totient function** is the number of positive integers from 1 to n which are coprime with n,

$$\phi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) \tag{A.13}$$

$J_k(n)$ **Jordan's totient function of order** $k > 0$ is the number of tuples $(a_1, \ldots, a_k)$ of k positive integers from 1 to n, the greatest common divisor of which is coprime with n,

$$J_k(n) = n^k \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p^k}\right), \tag{A.14}$$

in particular, $J_1 = \phi$.

For a proof of the formulas (A.10) – (A.14), it is sufficient to check them for the case that n is a power of a prime, and to use the multiplicativity property.

Proposition A.1 (Möbius inversion formula). Let f and g be arbitrary arithmetic functions. The equality

$$f(n) = \sum_{d|n} g(d)$$

holds for any $n \in \mathbb{N}$ if and only if one has

$$g(n) = \sum_{d|n} \mu(d) f(n/d)$$

for any $n \in \mathbb{N}$. In other words, the equalities $f = g * \mathbb{1}$ and $g = f * \mu$ are equivalent.

Proposition A.2. Let f be a multiplicative arithmetic function. Then the equality

$$\sum_{d|n} \mu(d) f(d) = \prod_{\substack{p|n \\ p \text{ prime}}} (1 - f(p)) \tag{A.15}$$

holds for any $n \in \mathbb{N}$.

Proof. Consider the function $g(n) = \sum_{d|n} \mu(d) f(d) = (\mu \cdot f) * \mathbb{1}$. It is multiplicative as the Dirichlet convolution of two multiplicative functions $\mu \cdot f$ and $\mathbb{1}$. Further,

$$g(p^\alpha) = \mu(1)f(1) + \mu(p)f(p) + \cdots + \mu(p^\alpha)f(p^\alpha) = 1 \cdot 1 + (-1) \cdot f(p) = 1 - f(p)$$

for each power of a prime p. Therefore,

$$g(n) = g(p_1^{\alpha_1}) \cdots g(p_r^{\alpha_r}) = (1 - f(p_1)) \cdots (1 - f(p_r))$$

for any natural n with prime factorization $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. □

From this proposition for $f(n) = 1/n^k$ we obtain the equality

$$\sum_{d|n} \frac{\mu(d)}{d^k} = \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p^k}\right). \tag{A.16}$$

The following relations can be proved directly by definition of the Dirichlet convolution or by using the multiplicativity property:

$$\mathbb{1} * \mathbb{1} = \tau \tag{A.17}$$

$$\mathbb{1} * \mathrm{id}_k = \sigma_k \tag{A.18}$$

$$\mathbb{1} * \mu = \varepsilon \tag{A.19}$$

$$\mathbb{1} * \phi = \mathrm{id} \tag{A.20}$$

$$\mathbb{1} * J_k = \mathrm{id}_k \tag{A.21}$$

$$\mathrm{id}_k * \mathrm{id}_\ell = \sigma_{k-\ell} \cdot \mathrm{id}_\ell \tag{A.22}$$

$$\mathrm{id}_k * \mu = J_k \tag{A.23}$$

$$\mu * \sigma_k = \mathrm{id}_k \tag{A.24}$$

$$\tau * \phi = \sigma \tag{A.25}$$

$$(\mathrm{id} \cdot \mu) * \sigma = \mathbb{1} \tag{A.26}$$

$$(\mathrm{id} \cdot \mu) * \phi = \mu. \tag{A.27}$$

For instance, to show the equality (A.26) one considers the function $f = (\mathrm{id}\cdot\mu) * \sigma$, which is multiplicative as well as the functions $\mathrm{id}\cdot\mu$ and σ. If p is a prime number, then

$$\begin{aligned} f(p^\alpha) &= \sum_{d|p^\alpha} d\mu(d)\sigma(p^\alpha/d) = \sum_{k=0}^{\alpha} p^k\mu(p^k)\sigma(p^{\alpha-k}) = 1\cdot\mu(1)\sigma(p^\alpha) + p\cdot\mu(p)\sigma(p^{\alpha-1}) \\ &= (1+p+\cdots+p^\alpha) - p(1+p+\cdots+p^{\alpha-1}) = 1, \end{aligned}$$

from where $f(n) = f(p_1^{\alpha_1})\cdots f(p_r^{\alpha_r}) = 1$ for any $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$.

The following statement is given in the textbook of Hardy and Wright [6, 316].

Proposition A.3. If an arithmetic function $f(n)$ is multiplicative and $f(p^\alpha) \to 0$ as $p^\alpha \to +\infty$, where p^α is a power of a prime, then $f(n) \to 0$ as $n \to +\infty$.

An arithmetic function f is **completely multiplicative**, if $f(mn) = f(m)f(n)$ for any positive integers m and n (not just coprime).

Proposition A.4. If a function f is completely multiplicative, then

$$f\cdot(g*h) = (f\cdot g)*(f\cdot h)$$

for any functions $g, h \in \mathcal{F}$.

Proof. Since f is completely multiplicative, then $f(n) = f(d)f(n/d)$ for any positive integer n and any of its divisor d. Therefore,

$$f\cdot(g*h)(n) = f(n)\sum_{d|n} g(d)h(n/d) = \sum_{d|n} f(d)g(d)\,f(n/d)h(n/d) = (f\cdot g)*(f\cdot h)(n),$$

as required. □

The function id is multiplicative, so the equality (A.26) can be established, by Proposition A.4 and the Möbius inversion formula:

$$(\mathrm{id}\cdot\mu)*\sigma = \mathbb{1} \iff \mathrm{id}\cdot\left(\mu*\frac{\sigma}{\mathrm{id}}\right) = \mathbb{1} \iff \frac{\sigma}{\mathrm{id}}*\mu = \frac{\mathbb{1}}{\mathrm{id}} \iff \frac{\mathbb{1}}{\mathrm{id}}*\mathbb{1} = \frac{\sigma}{\mathrm{id}} \iff \mathbb{1}*\mathrm{id} = \sigma.$$

The last equality is obviously true.

In 1916, Srinivasa Ramanujan expressed discrete convolutions of sigma-functions of odd order via linear combinations of functions σ_k and $\mathrm{id}\cdot\sigma_k$ with rational coefficients. For instance, he proved the proposition bellow (*cf.* collected papers [13]).

Proposition A.5 (**Ramanujan's formulas**, 1916)**.** The following equalities

$$(\sigma \vartriangle \sigma)(n) = \frac{5}{12}\sigma_3(n) + \frac{1}{12}\sigma(n) - \frac{1}{2}n\sigma(n),$$

$$(\sigma \vartriangle \sigma_3)(n) = \frac{7}{80}\sigma_5(n) + \frac{1}{24}\sigma_3(n) - \frac{1}{240}\sigma(n) - \frac{1}{8}n\sigma_3(n)$$

hold for any natural n.

A.2 Partitions of a positive integer

A **partition** of a number $n \in \mathbb{N}$ is its presentation as a sum

$$n = a_1 + \dots + a_r \tag{A.28}$$

of positive integers $a_1, \dots, a_r \in \mathbb{N}$. Two sums that differ only in the order of their summands are considered to be the same partition.

Definition. The function $P(n)$ equal to the number of distinct partitions of n is called the **partition function**.

The values of $P(n)$ for the first 18 positive integers are given in Table A.1.

Table A.1: $P(n)$ for $n \in [\![1, 18]\!]$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$P(n)$	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176	231	297	385

The generating function of the sequence $\{P(n)\}_{n=0}^{\infty}$, where $P(0) = 1$, is the following infinite product:

$$F(x) = \prod_{k=1}^{\infty} \frac{1}{1 - x^k}. \tag{A.29}$$

Indeed, the equality (A.28) can be re-written as $n = \alpha_1 k_1 + \dots + \alpha_s k_s$, meaning that among $a_1, \dots, a_r$ there are exactly α_1 numbers k_1, α_2 numbers k_2, etc., exactly α_s numbers k_s with condition $k_1 < \dots < k_s$. Therefore,

$$\begin{aligned} F(x) &= \prod_{k=1}^{\infty} \frac{1}{1 - x^k} = \prod_{k=1}^{\infty} (1 + x^k + x^{2k} + \dots + x^{\alpha k} + \dots) = 1 + \sum_{\substack{s \in \mathbb{N} \\ \alpha_1, \dots, \alpha_s \in \mathbb{N} \\ k_1 < \dots < k_s \in \mathbb{N}}} x^{\alpha_1 k_1 + \dots + \alpha_s k_s} \\ &= \sum_{n=0}^{\infty} P(n) x^n. \end{aligned}$$

In their famous paper [5, 1918] the mathematicians Hardy and Ramanujan obtained the asymptotic estimate of the partition function:

$$P(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi \sqrt{\frac{2n}{3}}\right) \quad \text{as } n \to \infty. \tag{A.30}$$

Proposition A.6. The discrete convolution of the functions σ and P satisfies the equality

$$(\sigma \vartriangle P)(n) = nP(n) - \sigma(n)$$

for any positive integer n.

Proof. Take the natural logarithm of both sides of the equality (A.29)

$$\log(F(x)) = \sum_{k=1}^{\infty} \log\left(\frac{1}{1 - x^k}\right)$$

and differentiate the new equality:

$$\frac{F'(x)}{F(x)} = \sum_{k=1}^{\infty} \frac{k x^{k-1}}{(1 - x^k)^2}, \quad \text{from where} \quad xF'(x) = F(x) \sum_{k=1}^{\infty} \frac{k x^k}{1 - x^k}. \tag{A.31}$$

An infinite formal series of the form $\sum_{k=1}^{\infty} a_k \dfrac{x^k}{1-x^k}$ is called the **Lambert series** with coefficients $a_1, a_2, \dots$ (*cf.* the classical textbook by Knopp [10, §58]). As well known, the following relations hold for sigma-functions:

$$\sum_{k=1}^{\infty} k^m \frac{x^k}{1-x^k} = \sum_{n=1}^{\infty} \sigma_m(n) x^n \tag{A.32}$$

for any nonnegative integer m. In particular, when $m = 1$ we get

$$\sum_{k=1}^{\infty} \frac{kx^k}{1-x^k} = \sum_{n=1}^{\infty} \sigma(n) x^n.$$

Because $F(x) = \sum_{n=0}^{\infty} P(n)x^n$, then $xF'(x) = \sum_{n=1}^{\infty} nP(n)x^n$ and we can write the equality (A.31) as

$$\sum_{n=1}^{\infty} nP(n)x^n = \left(\sum_{n=0}^{\infty} P(n)x^n\right)\left(\sum_{n=1}^{\infty} \sigma(n)x^n\right) = \sum_{n=1}^{\infty}\left(\sum_{k=0}^{n-1} P(k)\sigma(n-k)\right)x^n$$

$$= \sum_{n=1}^{\infty} \big(\sigma(n) + (\sigma \vartriangle P)(n)\big)x^n.$$

Comparing the coefficients of x^n leads to the relation $(\sigma \vartriangle P)(n) = nP(n) - \sigma(n)$. □

A.3 Permutation groups

Let M and L be some sets (finite or infinite). The elements of a set will be also called **points**.

Injection from the set M to the set L is a map $f : M \hookrightarrow L$ with the property: $f(x) \neq f(y)$ for any $x \neq y$ from M. In other words, an injection sends distinct elements of M to *distinct* elements of L.

Surjection from the set M to the set L is a map $f : M \twoheadrightarrow L$ with the property: for any $z \in L$ there exists at least one $x \in M$ such that $z = f(x)$. In other words, under surjection the image of the set M is the whole set L.

Bijection from the set M to the set L is a map $f : M \to L$, which is injective and surjective at the same time. If a map f is a bijection, then the **inverse map** $f^{-1} : L \to M$ is defined, namely

$$\text{for any } z \in L \text{ we define} \qquad f^{-1}(z) = x, \qquad \text{where } x \in M \text{ such that } z = f(x).$$

The existence of such an element $x \in M$ follows from the surjectivity of f, and its uniqueness follows from the injectivity f.

Permutation of the set M is any bijection of the set M with itself.

For an explicit definition of a permutation $s : M \to M$, it is presented as a matrix $2 \times |M|$, where the first row consists of all elements of the set M in some order, and under each element there is its image for the action of s in the second row:

$$s = \begin{pmatrix} x_1 & \dots & x_n \\ s(x_1) & \dots & s(x_n) \end{pmatrix}.$$

For instance, the record $s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ means that $M = \{1, 2, 3\}$ and $s : 1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 2$.

Product of two permutations $s : M \to M$ and $t : M \to M$, denoted by $s \circ t$, is defined to be the composition of the maps:

$$(s \circ t)(x) = s(t(x)) \quad \text{for any element } x \in M.$$

The symbol of composition is often omitted, and one writes shortly st.

The product of permutations has group features:

(*identity element*) $s \circ \mathrm{id} = \mathrm{id} \circ s = s$ for any permutation $s : M \to M$, where id is **identity permutation** defined as

$$\mathrm{id}(x) = x \quad \text{for all } x \in M;$$

(*inverse element*) $s \circ s^{-1} = s^{-1} \circ s = \mathrm{id}$ for any permutation $s : M \to M$, where s^{-1} is the inverse map (*cf.* above):

$$\text{if} \quad s = \begin{pmatrix} x_1 & \dots & x_n \\ y_1 & \dots & y_n \end{pmatrix}, \text{ then } \quad s^{-1} = \begin{pmatrix} y_1 & \dots & y_n \\ x_1 & \dots & x_n \end{pmatrix};$$

(*associativity*) $s \circ (t \circ u) = (s \circ t) \circ u$ for any three permutations $s, t, u : M \to M$.

Symmetric group of the set M is the group of *all* permutations of M. It is denoted by $Sym(M)$.
If $M = \{1, 2, \dots, n\}$, then one uses the shortened designation S_n , its order of this group is $n!$.

Permutation group on the set M is an arbitrary subgroup of the symmetric group $Sym(M)$.

Degree of a permutation group on M is defined to be the cardinality of the set M.
For instance, the degree of the group S_n equals n.

Support of a permutation $s \in Sym(M)$ is the set of those elements of M, which move under the action of s. The support is denoted by

$$\mathrm{supp}\, s := \{x \in M \mid s(x) \neq x\}.$$

The set of all points, which are stabilized, is denoted by

$$\mathrm{fix}\, s := \{x \in M \mid s(x) = x\}$$

$$= M \smallsetminus \mathrm{supp}\, s.$$

Graph of permutations $s_1, \dots, s_g$ of the set M is the following g-colored directed graph (possibly with loops):

- its vertices are the elements of the set M,
- two vertices x and y of the graph are connected by a directed edge with the i^{th} color and the starting vertex at x if and only if $s_i(x) = y$.

The graph of permutations $s_1, \dots, s_g$ will be denoted by $\mathsf{Graph}(s_1, \dots, s_g)$. In Figure 20, one can see the graph of the permutations $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 5 & 7 \end{pmatrix}$ and $t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 3 & 2 & 7 & 4 & 6 \end{pmatrix}$.

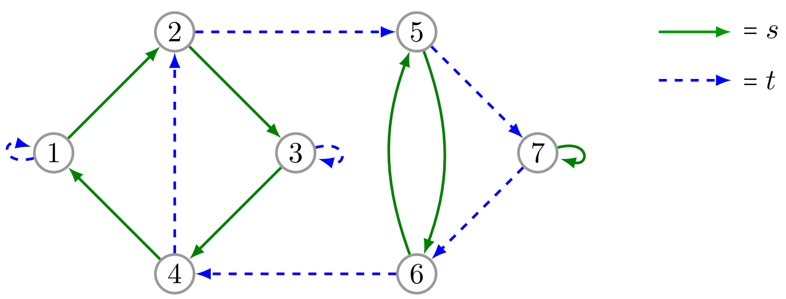

Figure 20: $\mathsf{Graph}(s, t)$

Cycle (k-cycle) on the set M is a permutation s that rearrange some k elements $x_1, \dots, x_k$ from M by the rule

$$s(x_1) = x_2, \quad s(x_2) = x_3, \quad \dots, \quad s(x_k) = x_1,$$

and the other elements don't move. In this case, one writes $s = (x_1 \ \dots \ x_k)$. The number k is called the **length** of the cycle.

Lemma A.1. Each permutation s of M is a product of disjoint cycles.

Proof. It suffices to consider the graph $\mathsf{Graph}(s)$ of the given permutation, and notice that distinct cycles of this graph correspond to disjoint cycles of the permutation s. For instance, from Figure 20 it follows that $s = (1\,2\,3\,4)(5\,6)$ and $t = (2\,5\,7\,6\,4)$. □

When presenting a permutation as a product of disjoint cycles, the cycles of length one are normally omitted (they correspond to the points which are stabilized by the permutation).

Cycle type of a permutation $s \in S_n$ is the formal expression $1^{l_1}2^{l_2}\dots k^{l_k}$ meaning that in the decomposition of s into disjoint cycles, there are exactly l_1 cycles of length 1, exactly l_2 cycles of length 2, and so on, exactly l_k cycles of length k. In particular, the following equality holds

$$l_1 + 2l_2 + \cdots + kl_k = n.$$

The cycle type of a permutation s will be denoted by $\mathsf{type}(s)$. For instance, if $s = (2\,3)(4\,5\,6\,7\,8)(10\,11) \in S_{15}$, then $\mathsf{type}(s) = 1^6 2^2 5^1$.

Two permutations has the same cycle type if and only if they are conjugate. This follows from the fact that when conjugating a cycle $(a_1\ a_2\ \dots\ a_k)$ of an arbitrary permutation s, one replaces the points a_i in the cycle by their images for the action of s:

$$s\,(a_1\ a_2\ \dots\ a_k)\,s^{-1} = (s(a_1)\ s(a_2)\ \dots\ s(a_k)).$$

Thus, any two cycles $(a_1\ a_2\ \dots\ a_k)$ and $(b_1\ b_2\ \dots\ b_k)$ of the same length are conjugate:

$$(b_1\ b_2\ \dots\ b_k) = \begin{pmatrix} a_1 & a_2 & \dots & a_k \\ b_1 & b_2 & \dots & b_k \end{pmatrix} (a_1\ a_2\ \dots\ a_k) \begin{pmatrix} a_1 & a_2 & \dots & a_k \\ b_1 & b_2 & \dots & b_k \end{pmatrix}^{-1}.$$

All permutations from S_n with the same cycle type form a **conjugacy class** of the group S_n.

Lemma A.2. The number of element in the conjugacy class $|C|$ of the group S_n corresponding to a cycle type $1^{l_1}2^{l_2}\dots k^{l_k}$ can be calculated via the formula

$$|C| = \frac{n!}{1^{l_1} l_1!\ 2^{l_2} l_2! \cdots k^{l_k} l_k!}. \tag{A.33}$$

Flag of a permutation $s \in S_n$ is a nondecreasing sequence $a_1 \le \dots \le a_r$ of positive integers, which are the lengths of the disjoint cycles in the decomposition of s (including the cycles of length 1). The next equality holds

$$a_1 + \cdots + a_r = n\,,$$

that is one gets a partition of n. The flag of the permutation s is denoted by $\mathsf{flag}(s)$. For instance, if $s = (2\,3)(4\,5\,6\,7\,8)(10\,11) \in S_{15}$, then $\mathsf{flag}(s) = 1,1,1,1,1,1,2,2,5$.

As well as for the cycle types, *two permutations have the same flag if and only if they are conjugate*. We conclude with the following statement:

Lemma A.3. The number of conjugacy classes in S_n is equal to $P(n)$.

Transposition is a cycle of length two. According to the relation (A.33), in the group S_n there are exactly $\frac{n!}{1^{n-2}(n-2)!\,2^1 1!} = \frac{n(n-1)}{2}$ transpositions.

Lemma A.4. Each permutation in S_n is a product of transposition (possibly intersecting).

Proof. Due to Lemma A.1, it suffices to prove the statement for an arbitrary cycle. But for cycles it is true, since $(x_1 \ \ldots \ x_k) = (x_1 \, x_2)(x_2 \, x_3)\ldots(x_{k-1} \, x_k)$ when $k > 1$. □

Even permutation is a permutation which is a product *even* number of transpositions. The other permutations are called **odd**. For instance, all cycles of odd length are even permutations, and cycles of even length are odd.

Signature of a permutation is defined to be 1 or −1 depending on whether the permutation is even or odd respectively. The signature of a permutations $s \in Sym(M)$ is denoted by $\mathrm{sign}(s)$:

$$\mathrm{sign}(s) = \begin{cases} 1, & \text{if } s \text{ is even;} \\ -1, & \text{if } s \text{ is odd.} \end{cases}$$

For instance, $\mathrm{sign}(\mathrm{id}) = \mathrm{sign}(1\ 2\ 3) = 1$ and $\mathrm{sign}(1\ 2) = -1$. For any permutations s and t the following relation holds:

$$\mathrm{sign}(s \circ t) = \mathrm{sign}(s) \cdot \mathrm{sign}(t).$$

Alternating group of the set M is the subgroup ofthose permutations from $Sym(M)$, which are products of *even* number of transpositions (that is the subgroup of all even permutations). It is denoted by $Alt(M)$, or shortly A_n for $M = \{1, 2, \ldots, n\}$. The order of A_n equals $^{n!}/_2$ when $n > 1$.

Transitive permutation group on the sets M is a subgroup $G \subseteq Sym(M)$ such that, for any points $x, y \in M$, there exists at least one permutation $s \in G$ sending x to y.

It easy to show that the group generated by permutation $s_1, \ldots, s_g$ is transitive if and only if the graph $\mathsf{Graph}(s_1, \ldots, s_g)$ is connected.

Block for a permutation group $G \subseteq Sym(M)$ is a *nonempty* subset $\Delta \subseteq M$ such that

$$s(\Delta) = \Delta \quad \text{or} \quad s(\Delta) \cap \Delta = \varnothing \qquad \text{for any permutation } s \in G.$$

Evidently, the subsets $\{x\}$ consisting of one element (*singletons*) and the whole set M are blocks for G. They are called **trivial**.

For example, for the Klein four-group $K_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \subset S_4$ there are exactly 11 blocks:

$$\{1\},\ \{2\},\ \{3\},\ \{4\},\ \{1,2,3,4\},\ \{1,2\},\ \{1,3\},\ \{1,4\},\ \{2,3\},\ \{2,4\},\ \{3,4\},$$

the first five of which are trivial.

Remark that if Δ is a block for a group G, then its image $s(\Delta)$ for the action of any permutation $s \in G$ is also a block for G.

Definition. A permutation group on M is said to be **primitive** if *all* blocks for it are trivial.

Let us show that for $|M| > 2$ *any primitive group $G \subseteq Sym(M)$ is automatically transitive.* Indeed, consider the orbit Δ of an arbitrary point $x \in M$ for the action of G, that is

$$\Delta = \{s(x) \mid s \in G\}.$$

Since $s(\Delta) = \Delta$ for any permutation $s \in G$, then Δ is a block, and so it is either a singleton or the whole set M. In the first case, we obtain $s(x) = x$ for all $s \in G$ and $x \in M$, that is the group G consists of the only permutation id. So, it cannot be primitive when $|M| > 2$. In the second case, the group G is transitive.

The converse is false: a transitive group is not always primitive. Remark, however, that *for a finite set M and a transitive group $G \subseteq Sym(M)$, the cardinality of any block Δ divides the cardinality of all set M*. Indeed, any two images $s_1(\Delta)$ and $s_2(\Delta)$ of the block for the action of permutations $s_1, s_2 \in G$

either coincide or don't intersect, by definition of a block. Besides, all images together cover the whole set M, since the group G is transitive. Hence, we get a partition of M,

$$M = s_1(\Delta) \sqcup \ldots \sqcup s_k(\Delta)$$

into several disjoint subsets, the cardinalities of which are equal to the cardinality of the block Δ. Thus $|\Delta|$ divides $|M|$. Moreover, each of these subset is also a block for G, from where follows the lemma below.

Lemma A.5. Consider a transitive permutation group $G \subseteq Sym(M)$ and some point $x \in M$. The group G is primitive if and only if the only blocks containing the point x are $\{x\}$ and M.

It is easy to check that for $|M| > 2$ the symmetric and the alternating groups of the set M are primitive. In 1873, the French mathematician Jordan [9] found a simple criterion whether a given *primitive* group coincides with $Alt(M)$ or $Sym(M)$.

Proposition A.7 (Jordan's theorem, 1873)**.** Let G be a primitive subgroup of S_n.

1. If G contains a transposition, then $G = S_n$.
2. If G contains a 3-cycle then, either $G = S_n$ or A_n.
3. In general, if G contains a cycle of prime order $p \leqslant n - 3$, then either $G = A_n$ or $G = S_n$.

A proof of this theorem can be found in the textbook of Wielandt [16, Theorem 13.9].

By means of Jordan's theorem, it is not difficult to obtain the following statement (see for example the paper by Isaacs and Zieschang [7]):

Proposition A.8. Let m and n be positive integers, $1 < m < n$. Two cycles $(1\ 2\ \ldots\ m)$ and $(1\ 2\ \ldots\ n)$ generate the group A_n if m and n are both odd, and the whole group S_n otherwise.

A.4 Representations of the symmetric group

Vector space over $\mathbb{C}$ is an additive group V together with a rule of multiplication $\lambda \cdot \vec{v}$ of elements $\vec{v} \in V$ by numbers $\lambda \in \mathbb{C}$. Moreover, the following axioms must be satisfied for any $\vec{u}, \vec{v} \in V$ and $\lambda, \mu \in \mathbb{C}$:

1) $1 \cdot \vec{v} = \vec{v}$,

2) $\lambda \cdot (\vec{u} + \vec{v}) = \lambda \cdot \vec{u} + \lambda \cdot \vec{v}$,

3) $(\lambda + \mu) \cdot \vec{v} = \lambda \cdot \vec{v} + \mu \cdot \vec{v}$,

4) $(\lambda\mu) \cdot \vec{v} = \lambda \cdot (\mu \cdot \vec{v})$.

Elements of the space V are called **vectors**, and the numbers from $\mathbb{C}$ are called **scalars**.

An example of a vector space over $\mathbb{C}$ is the set $\mathbb{C}^d$ of d-tuples of complex numbers, where $d \in \mathbb{N}$. Addition vector and multiplication by scalars are defined as

$$(x_1, x_2, \ldots, x_d) + (y_1, y_2, \ldots, y_d) = (x_1 + y_1, x_2 + y_2, \ldots, x_d + y_d),$$

$$\lambda \cdot (x_1, x_2, \ldots, x_d) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_d).$$

Subspace of a vector space V is any subset $U \subseteq V$ which is itself a vector space with rules of addition of vector and multiplication by scalars, inherited from V.

For a subset $U \subseteq V$ to be a subspace, it is necessary and sufficient that the following properties hold:

1) $\vec{0} \in U$,

2) if $\vec{u}$ and $\vec{v}$ lie in U, then their sum $\vec{u} + \vec{v}$ also lies in U,

3) if $\vec{v} \in U$, then also $\lambda \cdot \vec{v} \in U$ for any scalar $\lambda \in \mathbb{C}$.

The set $\{\vec{0}\}$ and the entire V are obviously subspaces in V, they are called the **trivial subspaces**. All other subspaces are called **proper**.

An example of a proper subspace in $\mathbb{C}^d$ for $d > 1$ is the set of d-tuples of complex numbers $(x_1, x_2, \ldots, x_d)$ with the condition $x_1 = 0$.

Matrix of size $d \times d$ is a square table having d rows and d columns and filled with numbers:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & & a_{2d} \\ \vdots & & \ddots & \vdots \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{pmatrix}$$

One writes shortly $A = (a_{ij})_{d \times d}$ or $A = (a_{ij})$, where a_{ij} is the element of the matrix at the intersection of the i^{th} row and the j^{th} column. A matrix is said to be **complex** if all its elements are complex (that is of the form $a + b\sqrt{-1}$ for some real numbers a and b).

The complex $d \times d$ matrices act on the vectors from the space $\mathbb{C}^d$ in the following way:

$$A \cdot \vec{v} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1d} \\ a_{21} & a_{22} & & a_{2d} \\ \vdots & & \ddots & \vdots \\ a_{d1} & a_{d2} & \cdots & a_{dd} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1d}x_d \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2d}x_d \\ \vdots \\ a_{d1}x_1 + a_{d2}x_2 + \cdots + a_{dd}x_d \end{pmatrix},$$

where a vector $\vec{v} \in \mathbb{C}^d$ is written as a column with d complex numbers. For instance,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

It is easy to check that for any vectors $\vec{u}, \vec{v} \in \mathbb{C}^d$ and scalars $\lambda, \mu \in \mathbb{C}$ the following equality holds:

$$A \cdot (\lambda\vec{u} + \mu\vec{v}) = \lambda \cdot (A \cdot \vec{u}) + \mu \cdot (A \cdot \vec{v}).$$

Identity matrix is a matrix with ones on the main diagonal (from the upper left corner to the lower right corner) and zeros everywhere else. The identity $d \times d$ matrix is denoted by I_d :

$$I_d = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Trace of a matrix is defined as the sum of the numbers on the main diagonal. The trace of a matrix A is denoted by $\mathrm{tr}(A)$:

$$\mathrm{tr}(A) = a_{11} + a_{22} + \cdots + a_{dd}\,.$$

For instance, $\mathrm{tr}(I_d) = d$.

Determinant of a $d \times d$ matrix is given by the following formula:

$$\det(A) = \sum_{s \in S_d} \mathrm{sign}(s) \cdot a_{1,s(1)}\, a_{2,s(2)}\, \ldots\, a_{d,s(d)}\,, \tag{A.34}$$

where one sums all products of d elements of the matrix, no two of which are in the same row or the same column. In a product $a_{1,s(1)}a_{2,s(2)} \cdots a_{d,s(d)}$ the first multiplier lies in the column $s(1)$, the second multiplier lies in the column $s(2)$ and so on, where s is some permutation of the numbers from 1 to d. In the sum, such a product is counted with a coefficient +1 or −1 depending on the parity of s (recall that $\mathrm{sign}(s)$ denotes the signature of the permutation).

For instance, for the 2×2 matrices one has

$$\mathrm{tr}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + d \qquad \text{and} \qquad \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc\,.$$

Product of matrices $A = (a_{ij})_{d\times d}$ and $B = (a_{ij})_{d\times d}$ is the $d \times d$ matrix with the element $\sum_{k=1}^{d} a_{ik}b_{kj}$ at the intersection of the i^{th} row and the j^{th} column:

$$A \cdot B = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} + \cdots a_{1d}b_{d1} & a_{11}b_{12} + a_{12}b_{22} + \cdots a_{1d}b_{d2} & \cdots & a_{11}b_{1d} + a_{12}b_{2d} + \cdots a_{1d}b_{dd} \\ a_{21}b_{11} + a_{22}b_{21} + \cdots a_{2d}b_{d1} & a_{21}b_{12} + a_{22}b_{22} + \cdots a_{2d}b_{d2} & & a_{21}b_{1d} + a_{22}b_{2d} + \cdots a_{2d}b_{dd} \\ \vdots & & \ddots & \vdots \\ a_{d1}b_{11} + a_{d2}b_{21} + \cdots a_{dd}b_{d1} & a_{d1}b_{12} + a_{d2}b_{22} + \cdots a_{dd}b_{d2} & \cdots & a_{d1}b_{1d} + a_{d2}b_{2d} + \cdots a_{dd}b_{dd} \end{pmatrix}.$$

In some sense, when multiplying two matrices "the rows of the first matrix are multiplied by the columns of the second matrix". The product of two matrices is not always commutative. For instance,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \text{but} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

The product of matrices has the following properties:

a. For any $d \times d$ matrix A one has the equality

$$A \cdot I_d = I_d \cdot A = A$$

b. If $\det(A) \neq 0$, then there exists a (unique) matrix denoted by A^{-1} such that

$$A \cdot A^{-1} = A^{-1} \cdot A = I_d$$

Such a matrix is called the **inverse of** A.

c. For any three $d \times d$ matrices A, B and C, one has the equality

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C$$

d. The determinant of a product equals a product of the determinants,

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

In view of these properties, all complex $d \times d$ matrices with *nonzero* determinant form a group, which is called the **general linear group** and denoted by $\mathrm{GL}_d(\mathbb{C})$.

$$\mathrm{GL}_d(\mathbb{C}) := \{A = (a_{ij})_{d\times d} \mid a_{ij} \in \mathbb{C} \ \text{ and } \ \det(A) \neq 0\}\,.$$

Homomorphism from a group G to a group K is a map $f : G \to K$ such that

$$f(g_1 g_2) = f(g_1) \cdot f(g_2) \qquad \text{for any } g_1, g_2 \in G.$$

In other words, under homomorphisms the image of a product (of two elements from G) is a product of their images (in K).

If a homomorphism f is moreover a bijection, then it is called an **isomorphism**. Isomorphism is a bijective homomorphism.

Representation of a group S_n is any homomorphism $\rho : S_n \to \mathrm{GL}_d(\mathbb{C})$, where $d \in \mathbb{N}$.

The natural number d is called the **dimension** of the representation ρ and denoted $\dim \rho$.

Given a representation $\rho : S_n \to \mathrm{GL}_d(\mathbb{C})$, to each permutation $s \in S_n$ corresponds a $d \times d$ complex matrix $\rho(s)$, so that the matrix of a product of two permutations $\rho(st)$ is equal to the product of matrices $\rho(s) \cdot \rho(t)$ for any $s, t \in S_n$.

Two representations $\rho : S_n \to \mathrm{GL}_d(\mathbb{C})$ and $\eta : S_n \to \mathrm{GL}_k(\mathbb{C})$ are said to be **equivalent** and one writes $\rho \sim \eta$, if $d = k$ and there exists a matrix $A \in \mathrm{GL}_d(\mathbb{C})$ such that

$$\rho(s) = A \cdot \eta(s) \cdot A^{-1} \qquad \text{for any permutation } s \in S_n\,.$$

Irreducible representation of the group S_n is such representation $\rho : S_n \to \mathrm{GL}_d(\mathbb{C})$, for which there is *no* proper subspace V of the vector space $\mathbb{C}^d$ with the property:

$$\rho(s) \cdot \vec{v} \in V \qquad \text{for any permutation } s \in S_n \text{ and any vector } \vec{v} \in V.$$

In other words, only the subspace $\{\vec{0}\}$ and the entire space $\mathbb{C}^d$ are invariant under the action of all matrices $\rho(s)$.

Lemma A.6. The number of pairwise nonequivalent irreducible representations of the group S_n is equal to the number of conjugacy classes in S_n, that is to the number of partitions of n.

Character of a representation ρ of S_n is the function $\chi_\rho : S_n \to \mathbb{C}$ such that

$$\chi_\rho(s) = \mathrm{tr}(\rho(s)) \qquad \text{for any permutation } s \in S_n.$$

This means that a character χ_ρ is given by a tuple of $n!$ complex numbers (possibly equal), which are the traces of the matrices $\rho(s)$ for $s \in S_n$. Here are some properties of the characters:

a. For any representation $\rho : S_n \to \mathrm{GL}_d(\mathbb{C})$, one has

$$\chi_\rho(\mathrm{id}) = \dim \rho\,.$$

Indeed, the homomorphism ρ sends the identity permutation id to the identity matrix I_d, that is $\chi_\rho(\mathrm{id}) = \mathrm{tr}(\rho(\mathrm{id})) = \mathrm{tr}(I_d) = d = \dim \rho$.

b. If permutations s and t are conjugate, then

$$\chi_\rho(s) = \chi_\rho(t).$$

This means that any character χ_ρ of the group S_n can take at most $P(n)$ distinct values, because at elements of each conjugacy class the same value (*cf.* Lemma A.3).

c. If representations ρ and η of the group S_n are equivalent, then their characters are equal:

$$\chi_\rho(s) = \chi_\eta(s) \qquad \text{for any permutation } s \in S_n\,.$$

d. For any representation $\rho : S_n \to \mathrm{GL}_d(\mathbb{C})$ and any permutations $s \in S_n$ the value of the character $\chi_\rho(s)$ is *integer*. This can be proved by means of Galois theory.

According to Lemma A.6 the groups S_2, S_3 and S_4 have respectively $P(2) = 2$, $P(3) = 3$ and $P(4) = 5$ pairwise nonequivalent irreducible representations. In the tables below, one finds the characters of those representations, where in the first row we indicated permutations from distinct conjugacy classes of S_n, in the second row – the number of permutations in those classes, and in the other rows – the values of the characters at those permutations.

Table A.2: The characters of the irreducible representations of S_2 and S_3.

C	id	(1 2)
$\lvert C\rvert$	1	1
χ_1	1	1
χ_2	1	−1

C	id	(1 2)	(1 2 3)
$\lvert C\rvert$	1	3	2
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	0	−1

Table A.3: The characters of the irreducible representations of the group S_4.

C	id	(1 2)	(1 2 3)	(1 2)(3 4)	(1 2 3 4)
$\lvert C\rvert$	1	6	8	3	6
χ_1	1	1	1	1	1
χ_2	1	−1	1	1	−1
χ_3	2	0	−1	2	0
χ_4	3	1	0	−1	−1
χ_5	3	−1	0	−1	1

Proposition A.9 (**Frobenius's formula**). Consider an arbitrary permutation $w \in S_n$ and its conjugacy class C. The number of pairs of permutations s and t from S_n such that $\mathsf{type}([s,t]) = \mathsf{type}(w)$ is equal to

$$n! \cdot |C| \cdot \sum_\rho \frac{\chi_\rho(w)}{\dim \rho}\,,$$

where the sum is over all (pairwise nonequivalent) irreducible representations ρ of S_n.

For instance, if $w = (1\;2\;3)$ then according to the relation (A.33) the number of permutations conjugate to w is equal to $|C| = \frac{n!}{1^{n-3}(n-3)!\,3^1 1!} = \frac{n(n-1)(n-2)}{3}$. Therefore, the number of pairs $(s,t) \in S_n \times S_n$ with a 3-cycle commutator is equal to the expression

$$n! \cdot \frac{n(n-1)(n-2)}{3} \cdot \sum_\rho \frac{\chi_\rho((1\;2\;3))}{\dim \rho}\,.$$

A proof of the generalized Frobenius's formula can be found in the work [8] and in the survey [17].

A.5 Square-tiled surfaces

Definition. A **square-tiled surface**, or shortly an **origami**, is a finite collection of copies of the unitary Euclidian square together with a gluing of the edges:

- the right edge of each square is identified to the left edge of some square,

- the top edge of each square is identified to the bottom edge of some square.

The notion of square-tiled surfaces came into sight in 1970s through the works of William P. Thurston [14] and William A. Veech [15]. Nowadays, these objects are being actively studied.

Consider an arbitrary origami O with n squares. Number its squares by the integers from 1 to n. Then we will obtain a pair of permutations $(s,t) \in S_n \times S_n$ that indicates how the squares are glued in the horizontal and the vertical directions:

$$\begin{aligned} s(i) &= j, \quad \text{if the right edge of the } i^{\text{th}} \text{ square is glued to the left edge of the } j^{\text{th}} \text{ one,} \\ t(i) &= k, \quad \text{if the top edge of the } i^{\text{th}} \text{ square is glued to the bottom edge of the } k^{\text{th}} \text{ one.} \end{aligned}$$

Note that by definition, a square-tiled surface doesn't depend on the numbering of its squares. If we number them otherwise, then we will get another pair of permutations (s', t'), which is conjugate to (s,t):

$$s' = usu^{-1} \quad \text{and} \quad t' = utu^{-1} \qquad \text{for some } u \in S_n.$$

The origami corresponding to a given pair of permutations $(s,t) \in S_n \times S_n$ will be denoted by $O(s,t)$. The permutation group $G = \langle s,t \rangle$ generated by the pair (s,t) is called the **monodromy group** of the surface $O = O(s,t)$. One says that an origami is **connected** if its monodromy group is transitive. An origami is **primitive** if its monodromy group is primitive. The reader can find more information on origamis and their monodromy groups in the Ph.D. thesis of David Zmiaikou [18, 2011].

A.6 Lattices in $\mathbb{R}^2$

Basis of the space $\mathbb{R}^2$ is a pair of its vectors $\vec{v}_1$ and $\vec{v}_2$ such that any vector $\vec{w} \in \mathbb{R}^2$ can be presented as a linear combination

$$\vec{w} = r_1 \vec{v}_1 + r_2 \vec{v}_2$$

with real coefficients r_1 and r_2.

For instance, the vectors $\overrightarrow{(1,0)}$ and $\overrightarrow{(0,1)}$ form a basis for the space $\mathbb{R}^2$, which is called **canonical**. It is easy to show that a pair of vectors $\overrightarrow{(x_1,y_1)}$ and $\overrightarrow{(x_2,y_2)}$ is a basis for $\mathbb{R}^2$ if and only if the following determinant of the matrix of these vectors

$$\det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = x_1 y_2 - x_2 y_1$$

differs from zero.

Lattice generated by a basis $(\overrightarrow{v}_1, \overrightarrow{v}_2)$ is the set of linear combinations

$$a_1\overrightarrow{v}_1 + a_2\overrightarrow{v}_2$$

with *integer* coefficients a_1 and a_2.

We conclude that a lattice is an additive subgroup of $\mathbb{R}^2$ with two generators. As a simple example of a lattice, one has $\mathbb{Z}^2$. Note that two distinct bases can generate the same lattice. For instance,

$$\mathbb{Z}^2 = \left\{a_1\overrightarrow{(1,0)} + a_2\overrightarrow{(0,1)} \mid a_1, a_2 \in \mathbb{Z}\right\} = \left\{a_1\overrightarrow{(3,2)} + a_2\overrightarrow{(7,5)} \mid a_1, a_2 \in \mathbb{Z}\right\}.$$

By the way, a pair of vectors $\overrightarrow{(x_1, y_1)}$ and $\overrightarrow{(x_2, y_2)}$ with integer coordinates generate the lattice $\mathbb{Z}^2$ if and only if the determinant of the matrix for these vectors equals 1 or −1:

$$\det\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = \pm 1.$$

All integer 2×2 matrices with determinant 1 or −1 form the group, which is denoted by $\mathrm{GL}_2(\mathbb{Z})$.

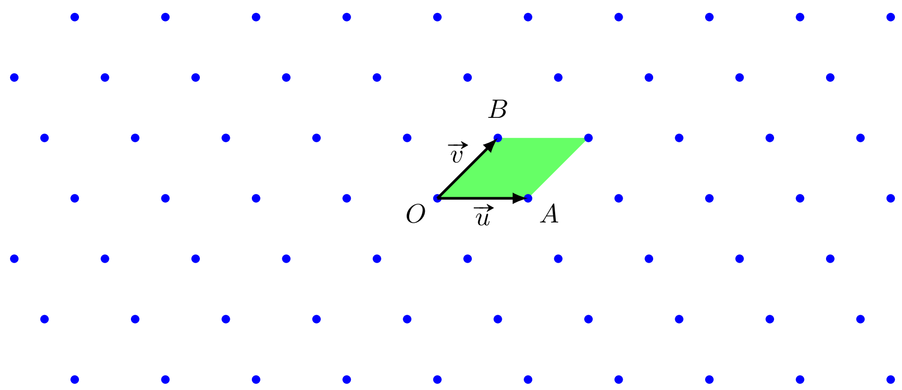

Figure 21: $\mathbb{R}^2$.

An arbitrary lattice $L \subset \mathbb{R}^2$ is usually illustrated in the real plane as a set of points: for each vector $\overrightarrow{(x, y)} \in L$ one draws the point with coordinates (x, y). Let us find a basis $(\overrightarrow{u}, \overrightarrow{v})$ for a lattice L as follows (*cf.* Figure 21):

- Let A be the closest lattice point to the origin of the plane O lying on the horizontal axis and having a positive first coordinate. Take $\overrightarrow{u} = \overrightarrow{OA}$.
- Let B be the lattice point such that the largest of the distances from it to the points O and A is the least (among all lattice points). Take $\overrightarrow{v} = \overrightarrow{OB}$.

It is not difficult to show that the basis $(\overrightarrow{u}, \overrightarrow{v})$ of $\mathbb{R}^2$, indeed, generates the lattice L. The parallelogram constructed on the vectors $\overrightarrow{u}$ and $\overrightarrow{v}$ is called the **fundamental parallelogram** of the lattice L.

A.7 Several useful sums

For any positive integer n, the following relations hold:

$$1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}=\frac{2n^3+3n^2+n}{6}, \tag{A.35}$$

$$1^3+2^3+\cdots+n^3=\frac{n^2(n+1)^2}{4}=\frac{n^4+2n^3+n^2}{4}, \tag{A.36}$$

$$1^4+2^4+\cdots+n^4=\frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}=\frac{6n^5+15n^4+10n^3-n}{30}. \tag{A.37}$$

In 1631, the German mathematician Faulhaber obtained a general formula for the sum of powers of the first n positive integers.

Using the formula (A.35), or else by induction, one can express the sum

$$\sum_{k=2}^{n} k(n-k)=\frac{(n+3)(n-1)(n-2)}{6}. \tag{A.38}$$

Let r be an arbitrary positive integer. The foolowing equality

$$\sum_{k=1}^{n} k(k-1)\cdots(k-r)=\frac{(n+1)n(n-1)\dots(n-r)}{r+2} \tag{A.39}$$

can be proved by induction on n. For $n=1$, it is trivially true. Suppose that it is true for n and show it for $n+1$:

$$\begin{aligned}\sum_{k=1}^{n+1} k(k-1)\cdots(k-r) &= (n+1)n\cdots(n-r+1)+\sum_{k=1}^{n} k(k-1)\cdots(k-r)\\ &= (n+1)n\cdots(n-r+1)+\frac{(n+1)n\cdots(n-r)}{r+2}\\ &= (n+1)n\cdots(n-r+1)\left(1+\frac{n-r}{r+2}\right)\\ &= \frac{(n+2)(n+1)n\cdots(n+1-r)}{r+2}.\end{aligned}$$

Thus, the equality (A.39) holds for any natural n.

The following infinite series is well-known:

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{n^2}+\cdots=\frac{\pi^2}{6}. \tag{A.40}$$

Let p_k denote the k^{th} prime number ($p_1=2$, $p_2=3$, $p_3=5$ and so on). Then by the formula for the sum of an infinite geometric progression,

$$\begin{aligned}\frac{1}{\prod_{k=1}^{\infty}\left(1-\frac{1}{p_k^2}\right)} &= \left(1+\frac{1}{p_1^2}+\cdots+\frac{1}{p_1^{2m}}+\cdots\right)\left(1+\frac{1}{p_2^2}+\cdots+\frac{1}{p_2^{2m}}+\cdots\right)\cdots\left(1+\frac{1}{p_k^2}+\cdots+\frac{1}{p_k^{2m}}+\cdots\right)\cdots\\ &= 1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{n^2}+\dots\end{aligned}$$

from where we get

$$\prod_{k=1}^{\infty}\left(1-\frac{1}{p_k^2}\right)=\frac{6}{\pi^2}\,. \tag{A.41}$$

Appendix B Programs (Sage)

B.1 Calculating $\#\mathcal{A}(n)$ and $\#\mathcal{B}(n)$ by Theorem A

```
# Calculating the cardinalities of A(n) and B(n) divided by n!
# and the probability #A(n)/#B(n) multiplied by P(n)/n,
# where P(n) is the partition function

def A(n):    # the cardinality of A(n) divided by n!
    A = 3*(n-2)*n*n*prod([1-1/(p*p) for p in prime_divisors(n)])/8
    return A

def B(n):    # the cardinality of B(n) divided by n!
    B = 0
    for k in range(1,n+1):
        B = B + ( sigma(k,3) - 2*k*sigma(k,1) + sigma(k,1) ) \
              * Partitions(n-k).cardinality()
    return 3*B/8

for n in range(3,256):
    a = A(n)
    b = B(n)
    proba = numerical_approx(Partitions(n).cardinality()*a/(n*b), digits=6)
    print n,a,b,proba
```

B.2 Calculating $\#\mathcal{A}_1(n)$, $\#\mathcal{B}_1(n)$, $\#\mathcal{A}_2(n)$ and $\#\mathcal{B}_2(n)$ by Theorem B

```
# Calculating the cardinalities of A1(n), B1(n), A2(n) and B2(n) divided by n!
# and the fractions #A1(n)/#B1(n)  and  n #A1(n)/#B1(n)

def A1(n):    # the cardinality of A1(n) divided by n!
    A1 = n*n*prod([1-1/(p*p) for p in prime_divisors(n)]) - 3*euler_phi(n)
    return n*A1/6

def B1(n):    # the cardinality of B1(n) divided by n!
    B1 = n*(n-1)*(n-2)/6
    return B1

def A2(n):    # the cardinality of A2(n) divided by n!
    A2 = A1(n) + (n+1)*(n-2)/2
    return A2

def B2(n):    # the cardinality of B2(n) divided by n!
    B2 = (n-1)*(n-2)*(n^2+5*n+12)/24
    return B2

for n in range(3,256):
    a1 = A1(n); a2 = A2(n)
    b1 = B1(n); b2 = B2(n)
    proba1 = numerical_approx(a1/b1, digits=6)
    proba2 = numerical_approx(n*a2/b2, digits=6)
    print n,a1,b1,proba1,a2,b2,proba2
```

B.3 The table for the first program

n	$\frac{\#\mathcal{A}(n)}{n!}$	$\frac{\#\mathcal{B}(n)}{n!}$	$\frac{P(n)}{n} \cdot \frac{\#\mathcal{A}(n)}{\#\mathcal{B}(n)}$
$n = 3$	3	3	1.00000
$n = 4$	9	12	0.937500
$n = 5$	27	42	0.900000
$n = 6$	36	99	0.666667
$n = 7$	90	231	0.834879
$n = 8$	108	462	0.642857
$n = 9$	189	882	0.714286
$n = 10$	216	1596	0.568421
$n = 11$	405	2772	0.743802
$n = 12$	360	4620	0.500000
$n = 13$	693	7524	0.715587
$n = 14$	648	11949	0.522937
$n = 15$	936	18480	0.594286
$n = 16$	1008	28182	0.516393
$n = 17$	1620	42108	0.672137
$n = 18$	1296	62139	0.446097
$n = 19$	2295	90216	0.656057
$n = 20$	1944	129690	0.469924
$n = 21$	2736	183876	0.561173
$n = 22$	2700	258720	0.475312
$n = 23$	4158	359667	0.630812
$n = 24$	3168	496650	0.418605
$n = 25$	5175	678942	0.596967
$n = 26$	4536	922824	0.460530
$n = 27$	6075	1243284	0.544727
$n = 28$	5616	1666434	0.447497
$n = 29$	8505	2216676	0.603969
$n = 30$	6048	2934960	0.384934
$n = 31$	10440	3860076	0.596934
$n = 32$	8640	5055468	0.445899
$n = 33$	11160	6582114	0.521136
$n = 34$	10368	8536704	0.439728
$n = 35$	14256	11013387	0.550426
$n = 36$	11016	14158620	0.388524
$n = 37$	17955	18115944	0.579588
$n = 38$	14580	23103531	0.432035
$n = 39$	18648	29339079	0.508238
$n = 40$	16416	37143414	0.412550
$n = 41$	24570	46842642	0.570360
$n = 42$	17280	58906848	0.371388
$n = 43$	28413	73816743	0.566278
$n = 44$	22680	92254470	0.420026
$n = 45$	27864	114926262	0.480236
$n = 46$	26136	142810932	0.419963
$n = 47$	37260	176935080	0.558966
$n = 48$	26496	218698536	0.371720
$n = 49$	41454	269577000	0.544565
$n = 50$	32400	331556148	0.399143
$n = 51$	42336	406749651	0.489689
$n = 52$	37800	497949144	0.411073
$n = 53$	53703	608155506	0.549707
$n = 54$	37908	741282927	0.365691
$n = 55$	57240	901553268	0.520940
$n = 56$	46656	1094417478	0.401052
$n = 57$	59400	1325794470	0.482739
$n = 58$	52920	1603220388	0.407041
$n = 59$	74385	1934935068	0.541996
$n = 60$	50112	2331328074	0.346238
$n = 61$	82305	2803785600	0.539700
$n = 62$	64800	3366550440	0.403639

$n = 63$	79056	4035301935	0.468165
$n = 64$	71424	4829450472	0.402460
$n = 65$	95256	5770461060	0.511113
$n = 66$	69120	6884707896	0.353444
$n = 67$	109395	8201402319	0.533481
$n = 68$	85536	9756209694	0.398106
$n = 69$	106128	11588746128	0.471741
$n = 70$	88128	13747002864	0.374382
$n = 71$	130410	16284447375	0.529809
$n = 72$	90720	19265466990	0.352699
$n = 73$	141858	22761858636	0.528094
$n = 74$	110808	26859653700	0.395234
$n = 75$	131400	31654953792	0.449320
$n = 76$	119880	37262223054	0.393222
$n = 77$	162000	43809552402	0.510005
$n = 78$	114912	51448804176	0.347403
$n = 79$	180180	60349988160	0.523371
$n = 80$	134784	70713852366	0.376361
$n = 81$	172773	82765353858	0.464001
$n = 82$	151200	96768892143	0.390741
$n = 83$	209223	113021049603	0.520528
$n = 84$	141696	131869111374	0.339544
$n = 85$	215136	153702652488	0.496764
$n = 86$	174636	178976363832	0.388745
$n = 87$	214200	208200528591	0.459865
$n = 88$	185760	241968535644	0.384795
$n = 89$	258390	280946616720	0.516650
$n = 90$	171072	325907179719	0.330309
$n = 91$	269136	377717284035	0.502002
$n = 92$	213840	437379463038	0.385463
$n = 93$	262080	506019158148	0.456722
$n = 94$	228528	584933843868	0.385161
$n = 95$	301320	675580163907	0.491329
$n = 96$	216576	779633241618	0.341784
$n = 97$	335160	898973004888	0.512081
$n = 98$	254016	1035756508248	0.375874
$n = 99$	314280	1192404057075	0.450542
$n = 100$	264600	1371686078070	0.367611
$n = 101$	378675	1576710505656	0.510014
$n = 102$	259200	1811027505411	0.338536
$n = 103$	401778	2078617830114	0.509029
$n = 104$	308448	2384020004256	0.379189
$n = 105$	355968	2732321142936	0.424746
$n = 106$	328536	3129309626520	0.380603
$n = 107$	450765	3581471185215	0.507146
$n = 108$	309096	4096172615898	0.337824
$n = 109$	476685	4681663620546	0.506245
$n = 110$	349920	5347299365100	0.361200
$n = 111$	447336	6103551249411	0.448927
$n = 112$	380160	6962273875326	0.371008
$n = 113$	531468	7936730093922	0.504520
$n = 114$	362880	9041912000331	0.335164
$n = 115$	536976	10294582596087	0.482668
$n = 116$	430920	11713663668234	0.377046
$n = 117$	521640	13320300598374	0.444400
$n = 118$	454140	15138327574623	0.376790
$n = 119$	606528	17194365434631	0.490192
$n = 120$	407808	19518380501214	0.321125
$n = 121$	647955	22143821814114	0.497235
$n = 122$	502200	25108295294676	0.375652
$n = 123$	609840	28453753086099	0.444743
$n = 124$	527040	32227301758050	0.374812
$n = 125$	691875	36481462023930	0.479913
$n = 126$	482112	41275139033940	0.326239
$n = 127$	756000	46673966702055	0.499171
$n = 128$	580608	52751476182174	0.374141

$n = 129$	704088	59589548978388	0.442882
$n = 130$	580608	67279817460768	0.356562
$n = 131$	830115	75924259717614	0.497810
$n = 132$	561600	85636879631886	0.328931
$n = 133$	848880	96544472830806	0.485686
$n = 134$	666468	108788647157883	0.372561
$n = 135$	775656	122526804400938	0.423714
$n = 136$	694656	137934560548434	0.370880
$n = 137$	950130	155207002394706	0.495886
$n = 138$	646272	174561588816615	0.329778
$n = 139$	992565	196239739104123	0.495274
$n = 140$	715392	220510316860680	0.349126
$n = 141$	920736	247671631144434	0.439535
$n = 142$	793800	278055607314156	0.370731
$n = 143$	1065960	312030305244999	0.487132
$n = 144$	736128	350004914182638	0.329218
$n = 145$	1081080	392432894620998	0.473237
$n = 146$	863136	439817967777015	0.369875
$n = 147$	1023120	492718025456790	0.429262
$n = 148$	898776	551752293927450	0.369259
$n = 149$	1223775	617606194024050	0.492409
$n = 150$	799200	691039911568743	0.314983
$n = 151$	1273950	772894401091422	0.491872
$n = 152$	972000	864101647122714	0.367701
$n = 153$	1174176	965692065073758	0.435260
$n = 154$	984960	1078806762045012	0.357832
$n = 155$	1321920	1204706649809355	0.470727
$n = 156$	931392	1344787094124012	0.325130
$n = 157$	1432665	1500589083803934	0.490326
$n = 158$	1095120	1673816743061772	0.367514
$n = 159$	1322568	1866350995369287	0.435268
$n = 160$	1092096	2080270461947106	0.352517
$n = 161$	1511136	2317868159571888	0.478471
$n = 162$	1049760	2581676436549903	0.326084
$n = 163$	1604043	2874487304423154	0.488870
$n = 164$	1224720	3199382197526328	0.366272
$n = 165$	1408320	3559756690115340	0.413341
$n = 166$	1270836	3959355961257543	0.366090
$n = 167$	1725570	4402304811032634	0.487945
$n = 168$	1147392	4893149912268492	0.318521
$n = 169$	1778049	5436896157324996	0.484627
$n = 170$	1306368	6039056997339408	0.349635
$n = 171$	1642680	6705698391579594	0.431752
$n = 172$	1413720	7443498705358386	0.364942
$n = 173$	1919133	8259801797584260	0.486620
$n = 174$	1300320	9162688266939000	0.323896
$n = 175$	1868400	10161039427496706	0.457236
$n = 176$	1503360	11264622040335510	0.361488
$n = 177$	1827000	12484165311019248	0.431691
$n = 178$	1568160	13831461547260159	0.364143
$n = 179$	2126655	15319458735881658	0.485365
$n = 180$	1384128	16962380066992416	0.310514
$n = 181$	2199015	18775835026110534	0.484961
$n = 182$	1632960	20776961284889271	0.354055
$n = 183$	2019960	22984557853851825	0.430621
$n = 184$	1729728	25419253353884082	0.362600
$n = 185$	2253096	28103665458294714	0.464481
$n = 186$	1589760	31062600353936955	0.322328
$n = 187$	2397600	34323243346612374	0.478146
$n = 188$	1848096	37915395208033464	0.362547
$n = 189$	2181168	41871699788260650	0.420943
$n = 190$	1827360	46227923813707419	0.346969
$n = 191$	2585520	51023228442343290	0.483042
$n = 192$	1751040	56300500326000918	0.321915
$n = 193$	2667888	62106675129029124	0.482677
$n = 194$	2032128	68493129084028803	0.361844

$n = 195$	2334528	75516064029414129	0.409153
$n = 196$	2053296	83236970116449534	0.354235
$n = 197$	2837835	91723083663501654	0.481965
$n = 198$	1905120	101047933645862742	0.318547
$n = 199$	2925450	111291885452415525	0.481617
$n = 200$	2138400	122542786024724076	0.346649
$n = 201$	2679336	134896609028552784	0.427714
$n = 202$	2295000	148458215846526687	0.360802
$n = 203$	3039120	163342120438969941	0.470573
$n = 204$	2094336	179673386486211618	0.319412
$n = 205$	3069360	197588533129562652	0.461117
$n = 206$	2434536	217236592093804140	0.360305
$n = 207$	2922480	238780179315327894	0.426116
$n = 208$	2491776	262396739637218088	0.357964
$n = 209$	3353400	288279813695479650	0.474681
$n = 210$	2156544	316640502633826371	0.300809
$n = 211$	3489255	347708964313511493	0.479637
$n = 212$	2653560	381736136035547706	0.359490
$n = 213$	3190320	418995500128643802	0.425991
$n = 214$	2730348	459785108688456483	0.359354
$n = 215$	3542616	504429665453630301	0.459617
$n = 216$	2496096	553282904139290952	0.319249
$n = 217$	3715200	606730041005201778	0.468465
$n = 218$	2886840	665190567041523327	0.358899
$n = 219$	3468528	729121134982345413	0.425185
$n = 220$	2825280	799018835131758714	0.341512
$n = 221$	3973536	875424591304180236	0.473653
$n = 222$	2708640	958927001865843087	0.318421
$n = 223$	4121208	1050166330936025529	0.477826
$n = 224$	3068928	1149839009723107200	0.350957
$n = 225$	3612600	1258702323871495356	0.407508
$n = 226$	3217536	1377579685178100327	0.358027
$n = 227$	4347675	1507366132665974724	0.477256
$n = 228$	2928960	1649034503019098316	0.317202
$n = 229$	4463955	1803641881580649222	0.476976
$n = 230$	3250368	1972336820806911186	0.342681
$n = 231$	3957120	2156366899923527676	0.411664
$n = 232$	3477600	2357087164124558250	0.357005
$n = 233$	4702698	2575968977502449760	0.476429
$n = 234$	3157056	2814609883916021835	0.315656
$n = 235$	4630176	3074743966840613277	0.456915
$n = 236$	3664440	3358253365177864734	0.356925
$n = 237$	4399200	3667180388444863818	0.422958
$n = 238$	3670272	4003740957196110207	0.348338
$n = 239$	5076540	4370338761889150869	0.475634
$n = 240$	3290112	4769580940928898822	0.304328
$n = 241$	5205420	5204294616553387620	0.475376
$n = 242$	3920400	5677545173275598931	0.353497
$n = 243$	4743603	6192655557546174948	0.422337
$n = 244$	4051080	6753227575531262298	0.356157
$n = 245$	5143824	7363164404629280352	0.446579
$n = 246$	3689280	8026695395935559994	0.316314
$n = 247$	5556600	8748402315038539272	0.470514
$n = 248$	4250880	9533248210691409798	0.355509
$n = 249$	5104008	10386607984040095500	0.421614
$n = 250$	4185000	11314301971302511335	0.341469
$n = 251$	5882625	12322631534338835217	0.474134
$n = 252$	3888000	13418418106425455256	0.309565
$n = 253$	5963760	14609044603394782002	0.469097
$n = 254$	4572288	15902500797767970771	0.355316
$n = 255$	5246208	17307431474208903984	0.402796
$n = 256$	4681728	18833189129072476098	0.355162

B.4 The table for the second program

n	$\frac{\#\mathcal{A}_1(n)}{n!}$	$\frac{\#\mathcal{B}_1(n)}{n!}$	$\frac{\#\mathcal{A}_1(n)}{\#\mathcal{B}_1(n)}$	$\frac{\#\mathcal{A}_2(n)}{n!}$	$\frac{\#\mathcal{B}_2(n)}{n!}$	$n \cdot \frac{\#\mathcal{A}_2(n)}{\#\mathcal{B}_2(n)}$	n
$n = 3$	1	1	1.00000	3	3	3.00000	$n = 3$
$n = 4$	4	4	1.00000	9	12	3.00000	$n = 4$
$n = 5$	10	10	1.00000	19	31	3.06452	$n = 5$
$n = 6$	18	20	0.900000	32	65	2.95385	$n = 6$
$n = 7$	35	35	1.00000	55	120	3.20833	$n = 7$
$n = 8$	48	56	0.857143	75	203	2.95567	$n = 8$
$n = 9$	81	84	0.964286	116	322	3.24224	$n = 9$
$n = 10$	100	120	0.833333	144	486	2.96296	$n = 10$
$n = 11$	165	165	1.00000	219	705	3.41702	$n = 11$
$n = 12$	168	220	0.763636	233	990	2.82424	$n = 12$
$n = 13$	286	286	1.00000	363	1353	3.48780	$n = 13$
$n = 14$	294	364	0.807692	384	1807	2.97510	$n = 14$
$n = 15$	420	455	0.923077	524	2366	3.32206	$n = 15$
$n = 16$	448	560	0.800000	567	3045	2.97931	$n = 16$
$n = 17$	680	680	1.00000	815	3860	3.58938	$n = 17$
$n = 18$	594	816	0.727941	746	4828	2.78128	$n = 18$
$n = 19$	969	969	1.00000	1139	5967	3.62678	$n = 19$
$n = 20$	880	1140	0.771930	1069	7296	2.93037	$n = 20$
$n = 21$	1218	1330	0.915789	1427	8835	3.39185	$n = 21$
$n = 22$	1210	1540	0.785714	1440	10605	2.98727	$n = 22$
$n = 23$	1771	1771	1.00000	2023	12628	3.68459	$n = 23$
$n = 24$	1440	2024	0.711462	1715	14927	2.75742	$n = 24$
$n = 25$	2250	2300	0.978261	2549	17526	3.63603	$n = 25$
$n = 26$	2028	2600	0.780000	2352	20450	2.99032	$n = 26$
$n = 27$	2673	2925	0.913846	3023	23725	3.44029	$n = 27$
$n = 28$	2520	3276	0.769231	2897	27378	2.96282	$n = 28$
$n = 29$	3654	3654	1.00000	4059	31437	3.74435	$n = 29$
$n = 30$	2760	4060	0.679803	3194	35931	2.66678	$n = 30$
$n = 31$	4495	4495	1.00000	4959	40890	3.75957	$n = 31$
$n = 32$	3840	4960	0.774194	4335	46345	2.99320	$n = 32$
$n = 33$	4950	5456	0.907258	5477	52328	3.45400	$n = 33$
$n = 34$	4624	5984	0.772727	5184	58872	2.99389	$n = 34$
$n = 35$	6300	6545	0.962567	6894	66011	3.65530	$n = 35$
$n = 36$	4968	7140	0.695798	5597	73780	2.73098	$n = 36$
$n = 37$	7770	7770	1.00000	8435	82215	3.79608	$n = 37$
$n = 38$	6498	8436	0.770270	7200	91353	2.99498	$n = 38$
$n = 39$	8268	9139	0.904694	9008	101232	3.47037	$n = 39$
$n = 40$	7360	9880	0.744939	8139	111891	2.90962	$n = 40$
$n = 41$	10660	10660	1.00000	11479	123370	3.81486	$n = 41$
$n = 42$	7812	11480	0.680488	8672	135710	2.68384	$n = 42$
$n = 43$	12341	12341	1.00000	13243	148953	3.82301	$n = 43$
$n = 44$	10120	13244	0.764120	11065	163142	2.98427	$n = 44$
$n = 45$	12420	14190	0.875264	13409	178321	3.38381	$n = 45$
$n = 46$	11638	15180	0.766667	12672	194535	2.99644	$n = 46$
$n = 47$	16215	16215	1.00000	17295	211830	3.83735	$n = 47$
$n = 48$	11904	17296	0.688252	13031	230253	2.71652	$n = 48$
$n = 49$	18179	18424	0.986702	19354	249852	3.79563	$n = 49$
$n = 50$	14500	19600	0.739796	15724	270676	2.90458	$n = 50$
$n = 51$	18768	20825	0.901224	20042	292775	3.49122	$n = 51$
$n = 52$	16848	22100	0.762353	18173	316200	2.98860	$n = 52$
$n = 53$	23426	23426	1.00000	24803	341003	3.85498	$n = 53$
$n = 54$	17010	24804	0.685776	18440	367237	2.71149	$n = 54$
$n = 55$	25300	26235	0.964361	26784	394956	3.72983	$n = 55$
$n = 56$	20832	27720	0.751515	22371	424215	2.95316	$n = 56$
$n = 57$	26334	29260	0.900000	27929	455070	3.49826	$n = 57$
$n = 58$	23548	30856	0.763158	25200	487578	2.99767	$n = 58$
$n = 59$	32509	32509	1.00000	34219	521797	3.86917	$n = 59$
$n = 60$	22560	34220	0.659264	24329	557786	2.61703	$n = 60$
$n = 61$	35990	35990	1.00000	37819	595605	3.87330	$n = 61$
$n = 62$	28830	37820	0.762295	30720	635315	2.99795	$n = 62$

$n = 63$	35154	39711	0.885246	37106	676978	3.45311	$n = 63$
$n = 64$	31744	41664	0.761905	33759	720657	2.99806	$n = 64$
$n = 65$	42120	43680	0.964286	44199	766416	3.74853	$n = 65$
$n = 66$	31020	45760	0.677885	33164	814320	2.68792	$n = 66$
$n = 67$	47905	47905	1.00000	50115	864435	3.88428	$n = 67$
$n = 68$	38080	50116	0.759837	40357	916828	2.99323	$n = 68$
$n = 69$	47058	52394	0.898156	49403	971567	3.50857	$n = 69$
$n = 70$	39480	54740	0.721228	41894	1028721	2.85070	$n = 70$
$n = 71$	57155	57155	1.00000	59639	1088360	3.89060	$n = 71$
$n = 72$	40608	59640	0.680885	43163	1150555	2.70108	$n = 72$
$n = 73$	62196	62196	1.00000	64823	1215378	3.89350	$n = 73$
$n = 74$	49284	64824	0.760274	51984	1282902	2.99853	$n = 74$
$n = 75$	58500	67525	0.866346	61274	1353201	3.39606	$n = 75$
$n = 76$	53352	70300	0.758919	56201	1426350	2.99455	$n = 76$
$n = 77$	71610	73150	0.978947	74535	1502425	3.81995	$n = 77$
$n = 78$	51480	76076	0.676692	54482	1581503	2.68706	$n = 78$
$n = 79$	79079	79079	1.00000	82159	1663662	3.90137	$n = 79$
$n = 80$	60160	82160	0.732230	63319	1748981	2.89627	$n = 80$
$n = 81$	76545	85320	0.897152	79784	1837540	3.51693	$n = 81$
$n = 82$	67240	88560	0.759259	70560	1929420	2.99879	$n = 82$
$n = 83$	91881	91881	1.00000	95283	2024703	3.90600	$n = 83$
$n = 84$	63504	95284	0.666471	66989	2123472	2.64994	$n = 84$
$n = 85$	95200	98770	0.963855	98769	2225811	3.77182	$n = 85$
$n = 86$	77658	102340	0.758824	81312	2331805	2.99889	$n = 86$
$n = 87$	95004	105995	0.896306	98744	2441540	3.51857	$n = 87$
$n = 88$	82720	109736	0.753809	86547	2555103	2.98076	$n = 88$
$n = 89$	113564	113564	1.00000	117479	2672582	3.91218	$n = 89$
$n = 90$	76680	117480	0.652707	80684	2794066	2.59892	$n = 90$
$n = 91$	119028	121485	0.979775	123122	2919645	3.83749	$n = 91$
$n = 92$	95128	125580	0.757509	99313	3049410	2.99625	$n = 92$
$n = 93$	116250	129766	0.895843	120527	3183453	3.52102	$n = 93$
$n = 94$	101614	134044	0.758065	105984	3321867	2.99907	$n = 94$
$n = 95$	133380	138415	0.963624	137844	3464746	3.77955	$n = 95$
$n = 96$	96768	142880	0.677268	101327	3612185	2.69294	$n = 96$
$n = 97$	147440	147440	1.00000	152095	3764280	3.91927	$n = 97$
$n = 98$	113190	152096	0.744201	117942	3921128	2.94770	$n = 98$
$n = 99$	139590	156849	0.889964	144440	4082827	3.50237	$n = 99$
$n = 100$	118000	161700	0.729746	122949	4249476	2.89327	$n = 100$
$n = 101$	166650	166650	1.00000	171699	4421175	3.92240	$n = 101$
$n = 102$	115872	171700	0.674851	121022	4598025	2.68468	$n = 102$
$n = 103$	176851	176851	1.00000	182103	4780128	3.92387	$n = 103$
$n = 104$	137280	182104	0.753855	142635	4967587	2.98617	$n = 104$
$n = 105$	158760	187460	0.846901	164219	5160506	3.34134	$n = 105$
$n = 106$	146068	192920	0.757143	151632	5358990	2.99926	$n = 106$
$n = 107$	198485	198485	1.00000	204155	5563145	3.92666	$n = 107$
$n = 108$	138024	204156	0.676071	143801	5773078	2.69016	$n = 108$
$n = 109$	209934	209934	1.00000	215819	5988897	3.92798	$n = 109$
$n = 110$	156200	215820	0.723751	162194	6210711	2.87267	$n = 110$
$n = 111$	198468	221815	0.894746	204572	6438630	3.52676	$n = 111$
$n = 112$	169344	227920	0.742998	175559	6672765	2.94670	$n = 112$
$n = 113$	234136	234136	1.00000	240463	6913228	3.93048	$n = 113$
$n = 114$	162108	240464	0.674147	168548	7160132	2.68354	$n = 114$
$n = 115$	237820	246905	0.963204	244374	7413591	3.79074	$n = 115$
$n = 116$	191632	253460	0.756064	198301	7673720	2.99762	$n = 116$
$n = 117$	231660	260130	0.890555	238445	7940635	3.51333	$n = 117$
$n = 118$	201898	266916	0.756410	208800	8214453	2.99940	$n = 118$
$n = 119$	268464	273819	0.980443	275484	8495292	3.85891	$n = 119$
$n = 120$	182400	280840	0.649480	189539	8783271	2.58955	$n = 120$
$n = 121$	286165	287980	0.993697	293424	9078510	3.91081	$n = 121$
$n = 122$	223260	295240	0.756198	230640	9381130	2.99943	$n = 122$
$n = 123$	270600	302621	0.894188	278102	9691253	3.52963	$n = 123$
$n = 124$	234360	310124	0.755698	241985	10009002	2.99792	$n = 124$
$n = 125$	306250	317750	0.963808	313999	10334501	3.79795	$n = 125$
$n = 126$	215460	325500	0.661936	223334	10667875	2.63783	$n = 126$
$n = 127$	333375	333375	1.00000	341375	11009250	3.93802	$n = 127$
$n = 128$	258048	341376	0.755906	266175	11358753	2.99948	$n = 128$

$n = 129$	312438	349504	0.893947	320693	11716512	3.53086	$n = 129$
$n = 130$	258960	357760	0.723837	267344	12082656	2.87641	$n = 130$
$n = 131$	366145	366145	1.00000	374659	12457315	3.93988	$n = 131$
$n = 132$	250800	374660	0.669407	259445	12840620	2.66706	$n = 132$
$n = 133$	375858	383306	0.980569	384635	13232703	3.86591	$n = 133$
$n = 134$	296274	392084	0.755639	305184	13633697	2.99953	$n = 134$
$n = 135$	345060	400995	0.860509	354104	14043736	3.40394	$n = 135$
$n = 136$	308992	410040	0.753565	318171	14462955	2.99187	$n = 136$
$n = 137$	419220	419220	1.00000	428535	14891490	3.94247	$n = 137$
$n = 138$	288420	428536	0.673036	297872	15329478	2.68152	$n = 138$
$n = 139$	437989	437989	1.00000	447579	15777057	3.94329	$n = 139$
$n = 140$	319200	447580	0.713169	328929	16234366	2.83658	$n = 140$
$n = 141$	408618	457310	0.893525	418487	16701545	3.53301	$n = 141$
$n = 142$	352870	467180	0.755319	362880	17178735	2.99958	$n = 142$
$n = 143$	471900	477191	0.988912	482052	17666078	3.90202	$n = 143$
$n = 144$	328320	487344	0.673693	338615	18163717	2.68450	$n = 144$
$n = 145$	479080	497640	0.962704	489519	18671796	3.80147	$n = 145$
$n = 146$	383688	508080	0.755172	394272	19190460	2.99960	$n = 146$
$n = 147$	454818	518665	0.876901	465548	19719855	3.47039	$n = 147$
$n = 148$	399600	529396	0.754822	410477	20260128	2.99853	$n = 148$
$n = 149$	540274	540274	1.00000	551299	20811427	3.94704	$n = 149$
$n = 150$	357000	551300	0.647560	368174	21373901	2.58381	$n = 150$
$n = 151$	562475	562475	1.00000	573799	21947700	3.94773	$n = 151$
$n = 152$	432288	573800	0.753377	443763	22532975	2.99348	$n = 152$
$n = 153$	521424	585276	0.890903	533051	23129878	3.52604	$n = 153$
$n = 154$	438900	596904	0.735294	450680	23738562	2.92371	$n = 154$
$n = 155$	585900	608685	0.962567	597834	24359181	3.80408	$n = 155$
$n = 156$	415584	620620	0.669627	427673	24991890	2.66955	$n = 156$
$n = 157$	632710	632710	1.00000	644955	25636845	3.94970	$n = 157$
$n = 158$	486798	644956	0.754777	499200	26294203	2.99966	$n = 158$
$n = 159$	587028	657359	0.893010	599588	26964122	3.53561	$n = 159$
$n = 160$	486400	669920	0.726057	499119	27646761	2.88855	$n = 160$
$n = 161$	669438	682640	0.980660	682317	28342280	3.87594	$n = 161$
$n = 162$	468018	695520	0.672904	481058	29050840	2.68259	$n = 162$
$n = 163$	708561	708561	1.00000	721763	29772603	3.95153	$n = 163$
$n = 164$	544480	721764	0.754374	557845	30507732	2.99880	$n = 164$
$n = 165$	627000	735130	0.852910	640529	31256391	3.38130	$n = 165$
$n = 166$	564898	748660	0.754545	578592	32018745	2.99969	$n = 166$
$n = 167$	762355	762355	1.00000	776215	32794960	3.95268	$n = 167$
$n = 168$	512064	776216	0.659693	526091	33585203	2.63161	$n = 168$
$n = 169$	786526	790244	0.995295	800721	34389642	3.93496	$n = 169$
$n = 170$	582080	804440	0.723584	596444	35208446	2.87986	$n = 170$
$n = 171$	729486	818805	0.890915	744020	36041785	3.53000	$n = 171$
$n = 172$	628488	833340	0.754180	643193	36889830	2.99891	$n = 172$
$n = 173$	848046	848046	1.00000	862923	37752753	3.95430	$n = 173$
$n = 174$	579768	862924	0.671865	594818	38630727	2.67917	$n = 174$
$n = 175$	829500	877975	0.944788	844724	39523926	3.74018	$n = 175$
$n = 176$	668800	893200	0.748768	684199	40432525	2.97827	$n = 176$
$n = 177$	811014	908600	0.892597	826589	41356700	3.53767	$n = 177$
$n = 178$	697048	924176	0.754237	712800	42296628	2.99973	$n = 178$
$n = 179$	939929	939929	1.00000	955859	43252487	3.95581	$n = 179$
$n = 180$	617760	955860	0.646287	633869	44224456	2.57994	$n = 180$
$n = 181$	971970	971970	1.00000	988259	45212715	3.95630	$n = 181$
$n = 182$	727272	988260	0.735912	743742	46217445	2.92879	$n = 182$
$n = 183$	896700	1004731	0.892478	913352	47238828	3.53826	$n = 183$
$n = 184$	769120	1021384	0.753017	785955	48277047	2.99554	$n = 184$
$n = 185$	999000	1038220	0.962224	1016019	49332286	3.81015	$n = 185$
$n = 186$	708660	1055240	0.671563	725864	50404730	2.67853	$n = 186$
$n = 187$	1062160	1072445	0.990410	1079550	51494565	3.92033	$n = 187$
$n = 188$	821560	1089836	0.753838	839137	52601978	2.99908	$n = 188$
$n = 189$	969570	1107414	0.875526	987335	53727157	3.47322	$n = 189$
$n = 190$	813960	1125180	0.723404	831914	54870291	2.88068	$n = 190$
$n = 191$	1143135	1143135	1.00000	1161279	56031570	3.95856	$n = 191$
$n = 192$	780288	1161280	0.671921	798623	57211185	2.68017	$n = 192$
$n = 193$	1179616	1179616	1.00000	1198143	58409328	3.95898	$n = 193$
$n = 194$	903264	1198144	0.753886	921984	59626192	2.99977	$n = 194$

$n = 195$	1038960	1216865	0.853801	1057874	60861971	3.38940	$n = 195$
$n = 196$	913752	1235780	0.739413	932861	62116860	2.94350	$n = 196$
$n = 197$	1254890	1254890	1.00000	1274195	63391055	3.95981	$n = 197$
$n = 198$	849420	1274196	0.666632	868922	64684753	2.65977	$n = 198$
$n = 199$	1293699	1293699	1.00000	1313399	65998152	3.96021	$n = 199$
$n = 200$	952000	1313400	0.724836	971899	67331451	2.88691	$n = 200$
$n = 201$	1189518	1333300	0.892161	1209617	68684850	3.53983	$n = 201$
$n = 202$	1020100	1353400	0.753731	1040400	70058550	2.99979	$n = 202$
$n = 203$	1347108	1373701	0.980641	1367610	71452753	3.88543	$n = 203$
$n = 204$	933504	1394204	0.669561	954209	72867662	2.67140	$n = 204$
$n = 205$	1361200	1414910	0.962040	1382109	74303481	3.81318	$n = 205$
$n = 206$	1082118	1435820	0.753659	1103232	75760415	2.99980	$n = 206$
$n = 207$	1297890	1456935	0.890836	1319210	77238670	3.53549	$n = 207$
$n = 208$	1108224	1478256	0.749683	1129751	78738453	2.98441	$n = 208$
$n = 209$	1485990	1499784	0.990803	1507725	80259972	3.92617	$n = 209$
$n = 210$	962640	1521520	0.632683	984584	81803436	2.52755	$n = 210$
$n = 211$	1543465	1543465	1.00000	1565619	83369055	3.96245	$n = 211$
$n = 212$	1179568	1565620	0.753419	1201933	84957040	2.99928	$n = 212$
$n = 213$	1416450	1587986	0.891979	1439027	86567603	3.54073	$n = 213$
$n = 214$	1213594	1610564	0.753521	1236384	88200957	2.99981	$n = 214$
$n = 215$	1571220	1633355	0.961959	1594224	89857316	3.81447	$n = 215$
$n = 216$	1111968	1656360	0.671332	1135187	91536895	2.67871	$n = 216$
$n = 217$	1647030	1679580	0.980620	1670465	93239910	3.88772	$n = 217$
$n = 218$	1283148	1703016	0.753456	1306800	94966578	2.99982	$n = 218$
$n = 219$	1540008	1726669	0.891895	1563878	96717117	3.54114	$n = 219$
$n = 220$	1258400	1750540	0.718864	1282489	98491746	2.86468	$n = 220$
$n = 221$	1760928	1774630	0.992279	1785237	100290685	3.93394	$n = 221$
$n = 222$	1206792	1798940	0.670835	1231322	102114155	2.67694	$n = 222$
$n = 223$	1823471	1823471	1.00000	1848223	103962378	3.96445	$n = 223$
$n = 224$	1365504	1848224	0.738820	1390479	105835577	2.94294	$n = 224$
$n = 225$	1606500	1873200	0.857623	1631699	107733976	3.40777	$n = 225$
$n = 226$	1430128	1898400	0.753333	1455552	109657800	2.99983	$n = 226$
$n = 227$	1923825	1923825	1.00000	1949475	111607275	3.96507	$n = 227$
$n = 228$	1305072	1949476	0.669448	1330949	113582628	2.67168	$n = 228$
$n = 229$	1975354	1975354	1.00000	2001459	115584087	3.96537	$n = 229$
$n = 230$	1447160	2001460	0.723052	1473494	117611881	2.88154	$n = 230$
$n = 231$	1760220	2027795	0.868046	1786784	119666240	3.44915	$n = 231$
$n = 232$	1546048	2054360	0.752569	1572843	121747395	2.99719	$n = 232$
$n = 233$	2081156	2081156	1.00000	2108183	123855578	3.96596	$n = 233$
$n = 234$	1406808	2108184	0.667308	1434068	125991022	2.66346	$n = 234$
$n = 235$	2053900	2135445	0.961814	2081394	128153961	3.81672	$n = 235$
$n = 236$	1628872	2162940	0.753082	1656601	130344630	2.99942	$n = 236$
$n = 237$	1953354	2190670	0.891670	1981319	132563265	3.54225	$n = 237$
$n = 238$	1633632	2218636	0.736323	1661834	134810103	2.93388	$n = 238$
$n = 239$	2246839	2246839	1.00000	2275279	137085382	3.96681	$n = 239$
$n = 240$	1466880	2275280	0.644703	1495559	139389341	2.57505	$n = 240$
$n = 241$	2303960	2303960	1.00000	2332879	141722220	3.96708	$n = 241$
$n = 242$	1743610	2332880	0.747407	1772770	144084260	2.97750	$n = 242$
$n = 243$	2106081	2362041	0.891636	2135483	146475703	3.54272	$n = 243$
$n = 244$	1800720	2391444	0.752984	1830365	148896792	2.99945	$n = 244$
$n = 245$	2284380	2421090	0.943534	2314269	151347771	3.74631	$n = 245$
$n = 246$	1643280	2450980	0.670458	1673414	153828885	2.67609	$n = 246$
$n = 247$	2463084	2481115	0.992733	2493464	156340380	3.93939	$n = 247$
$n = 248$	1889760	2511496	0.752444	1920387	158882503	2.99754	$n = 248$
$n = 249$	2266398	2542124	0.891537	2297273	161455502	3.54290	$n = 249$
$n = 250$	1862500	2573000	0.723863	1893624	164059626	2.88557	$n = 250$
$n = 251$	2604125	2604125	1.00000	2635499	166695125	3.96838	$n = 251$
$n = 252$	1732752	2635500	0.657466	1764377	169362250	2.62528	$n = 252$
$n = 253$	2643850	2667126	0.991273	2675727	172061253	3.93441	$n = 253$
$n = 254$	2032254	2699004	0.752964	2064384	174792387	2.99986	$n = 254$
$n = 255$	2333760	2731135	0.854502	2366144	177555906	3.39818	$n = 255$
$n = 256$	2080768	2763520	0.752941	2113407	180352065	2.99987	$n = 256$

References

[1] Tom M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, 1976.

[2] John D. Dixon, *The probability of generating the symmetric group*, Mathematische Zeitschrift **110** (1969), 199–205.

[3] Alex Eskin, Howard Masur, and Martin Schmoll, *Billiards in rectangles with barriers*, Duke Mathematical Journal **118** (2003), no. 3, 427–463.

[4] Alex Eskin and Andrei Okounkov, *Asymptotics of numbers of branched coverings of a torus and volumes of moduli spaces of holomorphic differentials*, Inventiones Mathematicae **145** (2001), 59–103.

[5] Godfrey H. Hardy and Srinivasa Ramanujan, *Asymptotic formulae in combinatory analysis*, Proceedings of the London Mathematical Society **s2-17** (1918), no. 1, 75–115.

[6] Godfrey H. Hardy and Edward M. Wright, *An introduction to the theory of numbers*, Oxford Press, USA, 1979.

[7] I. M. Isaacs and Thilo Zieschang, *Generating symmetric groups*, The American Mathematical Monthly **102** (1995), no. 8, 734–739.

[8] Gareth A. Jones, *Enumeration of homomorphisms and surface-coverings*, Quarterly Journal of Mathematics **46** (1995), no. 4, 485–507.

[9] Camille Jordan, *Sur la limite de transitivité des groupes non alternés*, Bulletin de la Société Mathématique de France **1** (1873), 40–71.

[10] Konrad Knopp, *Theory and application of infinite series*, Blackie & Son Limited, London and Glasgow, 1954.

[11] Samuel Lelièvre and Emmanuel Royer, *Orbitwise countings in $\mathcal{H}(2)$ and quasimodular forms*, International Mathematics Research Notices **2006** (2006), 30 pp., doi:10.1155/IMRN/2006/42151.

[12] Eugen Netto, *The theory of substitutions and its applications to algebra*, Ann Arbor, Michigan, 1892.

[13] Srinivasa Ramanujan, *On certain arithmetical functions*, Collected papers of Srinivasa Ramanujan (Godfrey H. Hardy, P. V. Seshu Aiyar, and Bertram M. Wilson, eds.), The University Press, Cambridge, 1927, pp. 136–162.

[14] William P. Thurston, *On the geometry and dynamics of diffeomorphisms of surfaces*, Bulletin of the American Mathematical Society **19** (1988), 417–431, (this paper was actually written around 1976).

[15] William A. Veech, *Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards*, Inventiones Mathematicae **97** (1989), no. 3, 553–583.

[16] Helmut Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.

[17] Don Zagier, *Applications of the representation theory of finite groups*, Appendix to S. Lando and A. Zvonkin, Graphs on Surfaces and Their Applications, Encyclopaedia of Mathematical Sciences 141, Springer-Verlag, Berlin Heidelberg, 2004, pp. 399–427.

[18] David Zmiaikou, *Origamis and permutation groups*, Ph.D. thesis, University Paris-Sud, France, 2011.

[19] Anton Zorich, *Flat surfaces*, Frontiers in Number Theory, Physics, and Geometry I: On Random Matrices, Zeta Functions, and Dynamical Systems (P. Cartier, B. Julia, P. Moussa, and P. Vanhove, eds.), vol. I, Springer-Verlag, 2nd ed., 2006, pp. 437–583.