Topology and statistics
of arithmetic and algebraic formulae

V.I. Arnold

Introduction

Topologic objects are usually spaces and manifolds, curves and surfaces. But topology might also study the peculiarities of the formulae and of the theories, instead of that of the points and of the spaces.

Working last year on the arithmetics of quadratic forms (and on its relations to the de Sitter relativistic world, [5]) I had discovered the topologic nature of many events in number theory (like the palindromic property of the continued fractions for $\sqrt{m/n}$, which ought to be known to Galois) as well as some strange statistic properties of the simplest arithmetic objects (and of their weak asymptotics, introduced in [6]).

While these statistic properties and these topologic phenomenae remain mostly experimental facts (being confirmed only by few millions of observations), I shall describe some of these discoveries, of which only a smaller fraction is at present proven as mathematical theorems (in the articles [1]-[5]). This number theory domain is strongly related to ergodic theory of dynamical systems.

I would like to thank R. Uribe-Vargas who was kind enough to type this text for me.

1 Fermat-Euler dynamical system

The simplest topological event in number theory is the “small Fermat theorem”, generalized by Euler and describing the arithmetic properties of the residues modulo $n$ of the elements of a geometric progression, similar to the periodic sequence of the residues modulo 13 of the powers of 2,

$$\{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, 2, \ldots\}.$$

The Fermat’s observation was the periodicity of the sequence

$$\{a^t \pmod{n}\}, \quad (t = 0, 1, \ldots)$$

---

*Partially supported by RFBR, grant 02-01-00655.
†I would like to thank R. Uribe-Vargas who was kind enough to type this text for me.
for the case of prime values of \( n \). Euler’s generalization deals with the case of mutually prime \( a \) and \( n \), where \( n \) might be any integer.

An example of an (unsolved) statistical problem occurring already in this simple situation is the question on the growth rate of the strangely irregular values of the periods \( T(n) \) of the geometric progression (say, for \( \{2^t \pmod{n} \}, \ t = 0, 1, \ldots \), \( n \) being odd).

The \textit{averaged growth rate} is the \textit{weak asymptotics} defined in [6]. The initial observations \( (n \leq 500) \) show the \textit{linear average growth of the period} (the deviations being rather large to both sides):

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|}
\hline
n & 5 & 7 & 9 & 13 & 15 & 19 & 29 & 31 & 51 & 509 & 511 \\
\hline
T & 4 & 3 & 6 & 12 & 4 & 18 & 28 & 5 & 8 & 35 & 508 & 9 \\
\hline
\end{array}
\]

It is uneasy to understand the growth rate from this table.

The behavior is more regular for the averages (at least along some neighbourhoods of the values of the modulus \( n \)). For instance, consider the tens of odd numbers in each one of the subsequent intervals \( 1 \leq n \leq 19, 21 \leq n \leq 39, \ldots \). \textit{The sums of the corresponding tens of periods} \( T \) \textit{and that of the tens of modulus} \( n \) \textit{are}

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|}
\hline
\sum n & 100 & 300 & 500 & 700 & 900 \\
\sum T & 68 & 158 & 246 & 290 & 329 \\
\hline
\end{array}
\]

the ratio \( \sum T/\sum n \) declining from 0.5 to the more or less stationary value 0.3 while \( n \) becomes 9 times larger than the starting value \( n \sim 10 \).

For larger values of odd moduli, \( 1 \leq k \leq n \), the sums of the periods are, according to the calculation of F. Aicardi, equal to the “\( \sum T \)” numbers of the following table:

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|}
\hline
n & 9 & 109 & 509 & 1009 & 1509 & 2009 \\
\hline
\sum T & 15 & 1409 & 23607 & 82761 & 176016 & 302277 \\
\hline
\end{array}
\]

I had studied these numbers using the double logarithmic paper (similarly to the trick used by Kolmogorov to discover the degrees appearing in his turbulence laws).

The “mean values asymptotics” observed above correspond to the approximate empirical formula of the kind

\[ T \sim 1.4n^{4/5} \]

(which would imply the sums growth proportional to \( \sum \sim n^{9/5} \)), corresponding to the straight lines on the double logarithmic paper.

There is no \textit{proven} theorems on the \( T \) or \( \sum T \) behavior, and even the possibilities \( T \sim Cn \) or \( T \sim Cn/\log n \) are not excluded by the observed values. It would be important for the chaoticity study to show that \( T(n) \) is much larger than \( n^{1/2} \) (or that \( \sum T \) than \( n^{3/2} \)), as we shall discuss in section 2.
The “Topological aspect” of the small Fermat theorem is the following statement, belonging essentially to Euler (see the discussion in [1]). Consider the multiplicative group of the residues modulo $n$ which are relatively prime to $n$. I shall call this group Euler group and shall denote it by $\Gamma(n)$.

If $n = p$ is a prime, the Euler group $\Gamma(p)$ contains all the $p - 1$ nonzero residues. In the general case the number $\varphi(n)$ of elements of the Euler group is a rather peculiar function of $n$ (called Euler function by Gauss):

$$\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline
n & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
\hline
\varphi(n) & 1 & 1 & 2 & 2 & 4 & 2 & 6 & 4 & 6 & 4 & 10 & 4 \\
\hline
\end{array}$$

Denote by $p_k$ the (different) prime factors of the modulus $n$ and by $a_k$ their multiplicities. In these notations the Euler function value is

$$\varphi\left(\prod p_k^{a_k}\right) = \prod [(p_k - 1)p_k^{a_k - 1}].$$

The multiplication of all residues, forming $\Gamma(n)$, by one of them (say, by 2 if $n$ is odd) defines a permutation (say, $2*$) of the finite set $\Gamma(n)$, consisting of $\varphi(n)$ elements (being all the residues, relatively prime to $n$).

Euler’s observation (which is equivalent to the Fermat-Euler theorem, usually formulated differently) says:

**Euler Theorem.** The Young diagram of the permutation $(a*)$ (multiplying each element of the Euler group $\Gamma(n)$ by a fixed element $a$ of this group) is always rectangular (in other words, every cycle of this permutation has the same period, $T(n)$).

Denote by $N(n)$ the number of these cycles, which is the number of orbits of the “multiplication by a” Fermat-Euler dynamical system

$$(a*) : \Gamma(n) \rightarrow \Gamma(n).$$

We consider below for simplicity the case $a = 2$, $n$ being odd.

The whole area of the Young diagram of the permutation $(a*)$ being the value of the Euler function, we deduce from the rectangular form of the Young diagram, stated by Euler Theorem, the identity

$$\varphi(n) = T(n)N(n).$$

This identity implies that the period, $T(n)$, and the number of orbits, $N(n)$, are divisors of the Euler function’s value, $\varphi(n)$.

**Example.** For $n = 31$, $a = 2$, we find the values $\varphi(n) = 30$, $T(n) = 5$, $N(n) = 6$. The Young diagram (filled by the elements of the cycles of the $(2*)$ permutation of the residues (mod 31)) is a rectangle, formed by 6 orbits of length 5 each one:
The values of the periods $T(n)$ and of the number of orbits $N(n)$ for the multiplication by 2 operation on the residues modulo $n$ are presented for all odd numbers till 511 in [2]; for instance, these tables contain the examples

<table>
<thead>
<tr>
<th>$n$</th>
<th>37</th>
<th>65</th>
<th>129</th>
<th>229</th>
<th>381</th>
<th>509</th>
<th>511</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>36</td>
<td>12</td>
<td>14</td>
<td>76</td>
<td>14</td>
<td>508</td>
<td>9</td>
</tr>
<tr>
<td>$N$</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>3</td>
<td>18</td>
<td>1</td>
<td>48</td>
</tr>
</tbody>
</table>

The product $\varphi(n) = T(n)N(n)$ is growing in the average like $cn$, $c$ being

$$\frac{6}{\pi^2} = \frac{1}{\zeta(2)}.$$  

Namely, B.A. Venkov had proved the Cesaro mean asymptotics

$$\lim_{n \to \infty} \frac{\sum_{k=1}^{n} \varphi(k)}{\sum_{k=1}^{n} k} = \frac{6}{\pi^2}.$$  

The coefficient $c$ appears here as the probability of the non-reducibility of the fraction $p/q$ (similarly, the number $1/\zeta(m)$ being the probability of the absence of integral points on the interval joining 0 to an integral vector of an $m$-dimensional vector space).

The equality of this probability to $1/\zeta(m)$ follows from the Euler’s product formula

$$\prod_p \frac{1}{1 - 1/p^m} = \sum_{n=1}^{\infty} \frac{1}{n^m} \quad \text{(the product along all the primes $p$).}$$

The product formula had been invented for this goal, as it is explained in [1] (the probability of the divisibility of an integral vector of an $m$-dimensional space by $p$ being $1/p^m$ and non-divisibilities for different $p$ being independent).

The identity $\sum 1/n^2 = \pi^2/6$ (due to Euler) is a corollary of the Fourier series representation of the $2\pi$-periodic function, coinciding with $|x|$ for $|x| \leq \pi$.

According to [1], the averaged empirical growth rate of $N(n)$ corresponds to the approximate asymptotics $N \sim 0.67n^{2/5}$.

The sum of degrees $2/5 + 4/5$ of the averaged asymptotics for $N$ and for $T$ is greater than the degree 1 of the averaged asymptotics of their product $\varphi$. This fact does not contradict the
Euler rectangle formula $\varphi = NT$, since the average of the product differs from the product of the averages.

The inequality $2/5 + 4/5 > 1$ is some indication of the frequent alternation of the large deviations of $N(n)$ from the average to both directions (similar to the intermittency phenomena in turbulence theory and in hydrodynamics).

While some empirical “averaged asymptotics” of this number-theoretic intermittency are provided by the statistics of the examples, no theorem is known in this young domain. The empirical approximate mean frequencies $p_N$ of the values of the number of orbits $N = 1, 2, 4, 8$ and of $N \geq 10$ in a neighbourhood of a fixed value of the modulus $n$ (between 1 and 2000) are, according to [1],

$$p_1 \sim an^{-7/18}, \quad p_2 \sim bn^{-1/9}, \quad p_4 \sim cn^{1/3}, \quad p_8 \sim dn^{1/9}, \quad p_{\geq 10} \sim cn^1.$$

I see no a priory reasons for the rationality of these observed degrees (the rationalities of the Kolmogorov’s degrees in turbulence theory, and of the Leonardo da Vinci degrees preceding them, being explained in hydrodynamics by the self-similarities and by dimensions theory).

The values of $T(n)$ and $N(n)$ have been computed for the odd numbers $n = 2k + 1$, $k = 1, \ldots, 1000$ by F. Aicardi. Her results are shown in the bi-logarithmic scale, in section 10, pages 27 and 28.

These results suggest the empirical averaged asymptotics

$$T(n) \sim 0.94n^{0.834},$$

$$N(n) \sim 0.60n^{0.36},$$

$$\varphi(n) \sim cn^a$$

(for $n$ till $10^5$ the constants are $a = 0.9994$, $c = 0.612$, while $6/\pi^2 = 0.6079271$).

**Remark 1.** The coefficients on the above averaged asymptotics for $T(n)$ and for $N(n)$ differ slightly from the coefficients in the corresponding formulas at page 2 for $T$ and at page 4 for $N$.

This difference, due to the difference between the ranges of $n$, is compatible with the experimental uncertainty of Aicardi’s coefficient for $N$. However, for $T$ the difference between the coefficient 1.4 of the formula at page 2 and the Aicardi’s coefficient 0.94 requires some explanation which is yet unknown.

The observed quantities in the tables of appendix were rather $(\sum T)(n) = \sum_{k=1}^n T(k)$, $k = 2t + 1$ and $(\sum N)(n) = \sum_{k=1}^n N(k)$, $k = 2t + 1$. The lines of these figures suggest

$$(\sum T)(n) \sim 0.255n^{1.834} \text{ and } (\sum N)(n) \sim 0.223n^{1.36}.$$
2 Randomness of the residues for the geometric progressions of numbers

We shall discuss below some “randomness criteria”, invented for the evaluation of the randomness degree of observed quantities.

The large Lyapunov exponent of the multiplication by 2 operation suggests a fast exponential growth of the initial perturbation in the Fermat-Euler dynamical system. One might therefore expect the chaotical distribution of the residues of the geometric progression’s members (among all the \( \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \) or among the \( \varphi(n) \) residues belonging to the Euler group \( \Gamma(n) \), which are relatively prime to \( n \)).

However the observed statistics of the periods \( T(n) \) shows the incomplete chaoticity of the \( T(n) \) elements of an orbit, namely, some repulsion between the elements of the orbits is observed.

It depends on the fact that all the \( T(n) \) residues of the elements \( \{2^t : t = 1, 2, \ldots, T\} \) of the geometric progression \( \text{mod } n \) should be different (inside each period), since the first repetition of a residue would imply the repetition of all the sequence following it.

If the residues of the \( T \) members of the orbit would be independent random elements of the \( m \)-elements set (where \( m = n \) in the case of the study of the distribution of residues in \( \mathbb{Z}_n \), and \( m = \varphi(n) \) in the case of the study of the distribution of residues in the Euler group \( \Gamma(n) \)), in this randomized case the celebrated “birthdays coincidence” problem of probability theory would suggest for \( T(n) \) a value proportional to \( \sqrt{n} \), that is a much smaller value than the observed ones (\( \sim n \)).

Namely, the probability of the absence of any repetition among the \( T \) independent choices from \( m \) possibilities is small, while \( T \) is “not large”, and is close to 1, when \( T \) is “large”, while the transition of the probability from 0 to 1 occurs in a neighbourhood of a special critical value, \( T_* \sim \sqrt{2m} \) (unfortunately I had not seen the transition erf-asymptotics theorem in probability textbooks).

Indeed, the number of sequences of \( T \) subsequent choices of different elements from a set of \( m \) elements is given by \( m(m-1) \cdots (m-T+1) \), the total number of sequences of choices being \( m^T \).

Thus the probability of absence of repetition is

\[
p(T, m) = \prod_{k=0}^{T-1} \frac{m-k}{m} \sim e^{\sum \ln(1-k/m)} \sim e^{-\sum (k/m)} \sim e^{-T^2/2m}.
\]

The true degree of \( n \) in the asymptotic for the period \( T(n) \) is unknown even for the smoothened averaged weak asymptotics. But the empirical data of [1]-[3] suggest that this degree, even if it is smaller than 1, seems to be closer to 1 than to the value 1/2, provided by the chaoticity requirement.

Thus the observed period of the sequence of residues of the geometric progression is longer than the one which would correspond to the random choices of the subsequent residues. In
other words the residues of the elements of the geometric progressions are avoiding the close approaches to each other and are repulsing each other in this sense.

To measure this repulsion I calculated the mean distances between the neighbouring points of a $T$-element subset of a circle of length $L$, defining this mean distance in the following way (introduced in the school-children lecture [1]).

Denote by $x_i$ ($i = 1, \ldots, T$) the lengths of the arcs into which the $T$ points of our set divide the circle:

$$\sum x_i = L, \quad x_i \geq 0.$$ 

We calculate first the sum of the squares of the lengths of these arcs:

$$R = \sum x_i^2.$$ 

To eliminate the dependence on the scale $L$ of the circle, consider the “randomness parameter” $r$, equal to the dimensionless normalized sum of squares,

$$r = \frac{R}{L^2}$$

(such normalization is equivalent to the contraction of the circle to the standard one of length 1).

The minimal value of the randomness parameter $r$, equal to $1/T$, is obtained at the “arithmetic progression” of equidistant points, similar to an army line:

$$x_i = \frac{1}{T}, \quad \sum x_i^2 = T \left(\frac{1}{T}\right)^2 = \frac{1}{T}.$$ 

The maximal value of the randomness parameter is $r = 1$ attained at the cluster of identical points (all lengths of the arcs being 0, except one of length 1).

To understand it one interprets $r$ as the squared distance from the origin to the point $z = x/L$ of the ($T - 1$)-dimensional simplex $\{0 \leq z_i \leq 1 : \sum z_i = 1\}$ in the Euclidean $T$-space.

The minimum is attained at the center of the simplex, and the maximum at its vertices.

Independent random choices of the points on the circle correspond to the random distribution of the point $z$ along the simplex (equidistributed with respect to the Lebesgue measure).

The value of the randomness parameter for such “freedom liking” distribution is intermediate between the “army line” distribution (minimal level) and the “cluster” distribution (maximal level). To compare the randomness of the sets consisting of different numbers of points, I had normalized the randomness parameter $r$ once more, dividing it by its minimal value for a given number of points:

**Definition.** The *binormalized randomness parameter* is defined as

$$s = \frac{r}{r_{\text{min}}} = rT.$$
The binormalized randomness parameter army-line (minimal) value and cluster-distribution (maximal) value are
\[ s_{\text{min}} = 1 \leq s \leq s_{\text{max}} = T. \]

The subway ticket long calculation (see the school-children lecture [1]) provides the freedom liking value of the binormalized randomness parameter to be close to \( s = 2 \):
\[ s_* = 2T/(T + 1). \]

Smaller values of the binormalized randomness parameter than the freedom liking value \((1 \leq s \leq s_*)\) indicate some kind of the mutual repulsion of the particles of the set (the smaller values of \( s \) corresponding to stronger repulsion).

Larger values of the binormalized randomness parameter than the freedom liking value \((s_* \leq s \leq T)\) indicate the mutual attraction of the set of points.

The values of the randomness parameter for the residues of the elements of the geometric progressions had been calculated by F. Aicardi (see [1]-[3]) in a computer-assisted way. In most cases the observed values of the randomness parameter \( s \) are not far from the value 1.5 (some times being close to 1 and in few cases larger than 2). However there are no theorems — I’m only describing few thousands of experiments here.

I made similar randomness parameter calculations for some other sets, for instance for the residues of the first hundreds of prime numbers and for some arithmetic progressions of the residues. In both cases some repulsion had been observed (the measured values of the randomness parameter being smaller than the freedom liking value).

In the arithmetic progression case the resulting value of the randomness parameter depends sensitively of the length \( T \) of the segment of the progression which is measured. One can consider both the randomness parameter, averaged along some choices of \( T \), or the randomness parameter of the optimal segments of the arithmetic progression, choosing the length \( T \) according to the continued fraction of \( a/n \) for the sequence \( \{at + b \pmod{n}\}, 1 \leq t \leq T \).

One might hope to prove in this case the asymptotic formulae (at least for the weak, averaged asymptotics), using virtually the Kuzmin-Gauss theorem on the ergodic characteristics of the elements of the continued fractions of random real numbers.

The repulsion of residues of the elements of geometric progressions influences also the common distribution of the lengths of the arcs of the integral circle \((\mathbb{Z}_n \text{ or } \Gamma(n))\) subdivided by these repulsing residues.

The length \( k \) of the \( T \) arcs of the integral circle of length \( m \) may vary from the minimal value 1 to the maximal value \( m - (T - 1) \). If the \( T \) different integral points, dividing the circle into these arcs, are chosen randomly and independently of each other then the frequencies \( p_k \) of the realizations of different values of the arc-length \( k \) are proportional to the Pascal triangle numbers on a line at distance \( T - 2 \) from its side (see the proof in [3]):
\[ p_k = \frac{C^{T-2}_{m-1-k}}{C^{T-2}_{m-1}}. \]

Thus, for the choices of \( T = 4 \) points among the 8 points of the integral circle \( \mathbb{Z}_8 \) of length 8 \((m = 8)\) the frequencies of the arcs of lengths 1, 2, 3, 4 and 5 are proportional, respectively,
to $15 : 10 : 6 : 3 : 1$. Thus the arcs of length 4 are observed 5 times less frequently than those of length 1.

For the geometric progression \( \{2^t \mod 15\} \), considered as the subset \( \{1, 2, 4, 8\} \) of the circle of 8 points \( \Gamma(15) = \{1, 2, 4, 7, 8, 11, 13, 14\} \), the “distances” between the neighbouring points along the Euler group \( \Gamma(15) \) are \( \{1, 1, 2, 4\} \) (where we call “the distance along \( \Gamma \)” the number of arcs, free of elements of \( \Gamma \), between the points whose distance is measured).

Thus the arc of length 1 is encountered 2.5 times less frequently, than it should be if the residues of the elements of the geometric progressions were purely randomly chosen. It confirms the repulsion of the residues of geometric progressions.

The randomness parameter (the binormalized one) is in this case

\[
s = \frac{1 + 1 + 4 + 16}{8^2} \cdot 4 = \frac{22}{16} = 1.375,
\]

which is substantially smaller than the freedom liking value \( 2T/(T+1) = 1.6 \). The smallness of \( s \) confirms the repulsion of the residues once more.

### 3 Topology of the squaring iterations

We shall begin with an extremely general object which belongs rather to logic than to mathematics.

**Definition.** A *monad* is a mapping of a finite set to itself. The *graph of a monad* is the oriented graph, whose vertices are the elements of the finite set and whose edges lead each vertex directly to its image (where it is sent by the monad).

In other words, a *monad’s graph is an arbitrary oriented graph, in which from every vertex there starts exactly one edge.*

The residues of the geometric progressions \( \{2^t \mod n\} \), considered above, are closely related to some “Frobenius monads”, sending each element of a finite group (or of a finite ring) to its square, \( x \mapsto x^2 \).

**Example.** The squaring graph for the residues ring \( \mathbb{Z}_7 = \mathbb{Z}/7\mathbb{Z} \) consists of three connected components shown in Figure 1. For instance, \( 4^2 \equiv 2 \mod 7 \) and \( 5^2 \equiv 4 \mod 7 \).

![Figure 1: The squaring graph for the ring of residues \( \mathbb{Z}_7 \).](image)

**Theorem 1.** Every connected component of any monad consists of a cycle-attractor, framed by rooted trees (whose roots are points of the attractor cycle).
The length of the cycle may be equal to 1, as it is the case for the component \(\{1, 6\}\) above. For the third component the length of the cycle is 2.

Consider the squaring operation of the elements of a finite commutative group as a monad.

**Theorem 2.** Each connected component of the graph of the squaring monad of the elements of a finite commutative group is a cycle, framed homogeneously (by isomorphic trees attached to each of its vertices).

The framing tree has \(2^k\) vertices (including the root vertex, belonging to the attracting cycle), and this tree is the product of binary trees (defined below as well as the products of trees).

**Definition.** A binary tree \(T_{2^n}\) (having \(2^n\) vertices) consists of the root vertex and of \(n\) floors, such that to each vertex of the \(i\)-th floor there lead exactly two edges (from two vertices belonging to the \((i + 1)\)-th floor), for \(i = 1, 2, \ldots, n - 1\).

The root of a binary tree is also reached by exactly two oriented edges: one issued from the root itself and the other from the unique vertex of the first floor.

The proof of Theorem 2 is contained in the following calculations.

## 4 The algebra of rooted trees

**Definition.** The product of two monads is the mapping from the direct product of the sets transformed—to themselves—by these monads to itself, each component being transformed independently of the other by the corresponding monad:

\[
(X * Y)(x, y) = (Xx, Yy).
\]

The graph of the product \(X * Y\) is called the product of the corresponding two graphs, \((\text{graph } X) * (\text{graph } Y)\). Its set of vertices is the direct product of the set of vertices of the two multipliers-graphs.

Thus the number of vertices of the graph-product is the product of the number of vertices of the multipliers.

**Example.** The product \(A_n\) the cycle \(O_n\) of length \(n\) (having \(n\) vertices) with the simplest binary graph \(T_2 = A_1\) is a \(2n\)-vertex graph, whose attracting cycle \(O_n\) is framed at each of its vertices by the single-edge rooted tree (as it is the case for the third component

\[
A_2 = O_2 * A_1 = \{2, 3, 4, 5\}
\]

of the squaring graph for the ring of residues \(\mathbb{Z}_7\), shown above). The preceding component, \(\{1, 6\}\), is the \(A_1\) graph.

The rooted trees are connected graphs of their monads (whose cycle’s length equals 1). The graph of the product of such monads is itself a rooted tree.

**Definition.** The product of two rooted trees is the rooted tree of the product of their monads.
Example. \( A_1 \ast A_1 = D_1 \) is a 4-vertex rooted tree, whose root vertex is reached by the 3 edges issued from the other 3 vertices.

Example. The graph \( D_n = O_n \ast D_1 \) has \( 4n \) vertices and one attracting \( n \)-cycle, framed at each of its \( n \) vertices by three arriving edges (forming, together with the vertex of the cycle, the framing tree \( D_1 \) of this vertex).

Studying the products of rooted trees it is useful to associate to a tree the sequence of its ranks:

**Definition.** The rank \( r_i (i = 0, 1, \ldots) \) of a rooted tree is the number of vertices connected to the root by a path of length \( i \) (that is, consisting of \( i \) edges).

**Example.** \( r_0 = 1, r_1(D_1) = 3, r_1(T_4) = 1, r_2(T_4) = 2. \)

The ranks of the product are provided by the ranks multiplication formula:

\[
r_k(X \ast Y) = \sum_{\max(i,j)=k} r_i(X) \cdot r_j(Y).
\]

In other words, the ranks sums, \( s_k = r_0 + r_1 + \cdots + r_k \), are multiplicative:

\[
s_k(X \ast Y) = s_k(X) \ast s_k(Y).
\]

To compute the ranks of the product tree one write first the matrix of the products of the ranks of the multipliers-trees, and one add then the elements of this matrix along each hook bordering the \( i = j = 0 \) element of the matrix.

For the product of the binary trees \( T_4 \) and \( T_8 \) the matrix of the ranks products (together with its bordering hooks) is the matrix

\[
\begin{bmatrix}
2 & 2 & 4 & 8 \\
1 & 1 & 2 & 4 \\
1 & 1 & 2 & 4
\end{bmatrix},
\]

implying the following values of the product’s ranks:

\[ r_0 = 1, \ r_1 = 3, \ r_2 = 12, \ r_3 = 16. \]

Similarly the ranks of a binary tree multiplied by itself, \( T_2^n \ast T_2^n \), form the sequence

\[ 1, 3, 3 \cdot 4, 3 \cdot 4^2, \ldots, 3 \cdot 4^{n-1}, \]

(continued by the powers of 2, while one of the multipliers-trees is replaced by a larger binary tree).

I’m describing so many details on the products of binary trees, because they are the only homogeneously framing trees for the squaring graphs of the finite commutative groups.
This follows from the fact that any such group is a direct product of the cyclic ones, and that the graph of the multiplication by 2 (that is, of adding each element of the group to itself) is the union of unframed cycles for any odd order cyclic group (written additively).

Indeed, Euler’s Theorem implies that \(2^{\varphi(n)} \equiv 1 \pmod{n}\) for any odd number \(n\). Hence \(2^{\varphi(n)}a \equiv a \pmod{n}\), and thus any element \(a\) belongs to a cycle of the monad of the cyclic group, \(\mathbb{Z}_n\).

This table of multiplication of cycles is provided by the easily proved formula

\[O_m \ast O_n = dO_c,
\]

where \(d\) is the greatest common divisor of the numbers \(m\) and \(n\) and \(c\) their smallest common multiple.

The product with \(d\) in the formula above means the disjoint union of \(d\) copies (of cycles of equal length \(c\)).

For instance, in the algebra of graphs the following identities hold:

\[O_3 \ast O_5 = O_{15}, \quad O_6 \ast O_{10} = 2O_{30}.
\]

The graph of the doubling monad (of the addition of each element to itself) for the cyclic group of order \(2^n\) is the binary tree \(T_{2^n}\):

![The binary tree \(T_8\).](image)

Indeed, \(7 + 7 \equiv 6 \pmod{8}\), \(\{r_k\} = \{1, 1, 2, 4\}\) for the doubling monad of the group \(\mathbb{Z}_8\).

The algebra of graphs described above provides the proof of Theorem 2 together with easy calculations in more difficult situations. Consider, for instance, the Euler group \(\Gamma(125) \simeq \mathbb{Z}_{100}\), containing 100 elements. The largest component of the squaring monad’s graph (which is extremely useful for the study of the square residues mod 125) has for this group 80 vertices, the framed cycle being \(O_{20} \ast T_4\). Denoting its points by the corresponding residues (mod 125), belonging to the multiplicative group \(\Gamma(125)\) we get the largest component of the squaring graph (see Figure 3).

The oriented edges of this graph are leading to the quadratic residues modulo 125 (like \(13^2 \equiv 44 \pmod{125}\)), while the vertices far from the cycle (like 22, 37,...) are not quadratic residues (the congruences like \(x^2 \equiv 22 \pmod{125}\) are unsolvable). Unfortunately, these graphs of quadratic residues are missing in number theory books.
Figure 3: Graph of the largest component of the squaring monad of $\Gamma(125)$

The topology of such graphs explains many mysterious facts of the theory of quadratic forms like, say, the structure of semi-group of the set of values of the “perfect” quadratic forms, studied in [5] (for instance, the set of values of the quadratic form $x^2 + 2y^2$).

In this example the odd values of the form constitute the multiplicative semi-group of the numbers

$$n = \prod (p_i^{a_i} \cdot q_j^{b_j} \cdot r_{k}^{c_k} \cdot s_{l}^{d_l}),$$

where $p_i$, $q_j$, $r_k$ and $s_l$ denote the different primes whose residues (mod 8) are, respectively, 1, 3, 5 and 7. The multipliers $r \equiv 5 \pmod{8}$ and $s \equiv 7 \pmod{8}$ should have even degrees in $n$.

For instance, the numbers $n = 5, 7, 125, 343$ are not representable, while $n = 3, 17, 25, 49$ are representable by the form $x^2 + 2y^2$ on $\mathbb{Z}^2$ (like, $17 = 3^2 + 2 \cdot 2^2$).

In the examples studied till today the multiplicative semi-groups of values of perfect forms are defined by linear conditions on the degrees of different primes, while in general multiplicative semi-groups there might be also restrictions of the type of degrees inequalities. It is unknown whether inequalities restrictions from convex geometry would happen in the case of the semi-group of values of a perfect form.
Squaring operation graphs in permutation’s groups

Trying to extend the framing homogeneity theorem from the commutative groups to the general finite groups, I have discovered the following fact.

**Theorem 3.** Any connected component of the graph of the squaring operation in the symmetric group of permutations of $n$ elements (as well as in its subgroup of even permutations) is framed homogeneously (the framing trees of its vertices being mutually isomorphic).

This framing homogeneity result follows from the description of the permutations forming the attracting cycle of the group of permutations: the permutations forming the attractor-cycle are characterized by the property that each of their cycles has odd length.

Every cyclic permutation of odd length is conjugate to its square in the group of permutations.

This conjugation sends each vertex of the attractor-cycle to the next one, acting also on all vertices and sending the framing tree of the initial vertex of the attractor onto the tree framing the next vertex, permuting all framing trees along the cycle, which are thus isomorphic.

In the group of even permutations an odd order cycle like $(1, 2, 3)$ is not conjugate to its square $(1, 3, 2)$, the conjugating permutation $(2, 3)$ of three elements being odd.

However the odd permutation conjugation still defines an (exterior) automorphism, moving the attractor-cycle vertex to the next place, and sending the framing tree onto the next one, proving the homogeneity of the framing for the graph of the group of even permutations.

For instance, the group $SL(2, \mathbb{Z}_6)$ consists of 144 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, whose elements are residues mod 6, for which $ad - bc \equiv 1 \mod 6$.

The squaring graph consists of 14 components:

$$[\text{graph}(SL(2, \mathbb{Z}_6))] = T + (O_2 * R) + 4(O_2 * E_8) + 8A_2,$$

where the tree $T$ has ranks sums $s = (1, 8, 32)$ and the tree $R$ has ranks sums $s = (1, 2, 8)$.

Explicitly, the 16 matrices forming the graph $O_2 * R$ are shown in Figure 4.

In this component the homogeneity of the framing is explained by the (exterior) automorphism, conjugating each matrix by the orientation reversing mapping $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, sending $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\begin{pmatrix} d & c \\ b & a \end{pmatrix}$.

The number of matrices of any trace $a + d$ in every component is shown in the following table:

<table>
<thead>
<tr>
<th>Trace</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>24</td>
</tr>
<tr>
<td>5</td>
<td>24</td>
</tr>
<tr>
<td>6</td>
<td>16</td>
</tr>
</tbody>
</table>
Figure 4: The 16 matrices forming the graph $O_2 \ast R$.

<table>
<thead>
<tr>
<th>$a + d$\component</th>
<th>$T$</th>
<th>$O_2 \ast R$</th>
<th>$4(O_2 \ast E_8)$</th>
<th>$8A_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>$8 \cdot 2$</td>
</tr>
<tr>
<td>2</td>
<td>3+1</td>
<td>0</td>
<td>$3 \cdot (6 + 2)$ + 6</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>3+1</td>
<td>0</td>
<td>$3 \cdot 8 + (8 + 2)$</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>$8 \cdot 2$</td>
</tr>
</tbody>
</table>

Notations like $3 + 1$ at the place $(2, T)$ in the table mean that the 4 points having $a + d \equiv 2$ in $T$ are subdivided in two classes, one of 3 elements and the other of 1 element, occupying non-isomorphic places in the tree $T$ (these matrices are in this example, $\{\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}\}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, at distance 1 and 0 from the root).

It would be interesting to relate this structure of the squaring graph to the conjugacies and automorphisms acting on the group (they should preserve the graph).

I do not know to which degree does the topological structure of the graph of the non-direct product $P$ of finite groups $G, H$ reflect the algebraic non-directness for

$$1 \rightarrow H \rightarrow P \rightarrow G \rightarrow 1,$$

even for the two-fold covering case (where $H = \mathbb{Z}_2$) and for the case of subgroups of index 2 (where $G = \mathbb{Z}_2$, as for the subgroup $H$ of even permutations).

Non-isomorphic finite groups having isomorphic graphs of the squaring monads are also unknown to me.

6 Monads homogeneity for arbitrary finite groups

The morphisms preserving the monad structure, their groups and categories deserve special study.
Theorem 4. For any finite group, the framing of the attracting cycle of the squaring monad is homogeneous (the rooted trees attracted by the vertices of the cycle are all isomorphic along any connected component).

Proof. We shall construct a mapping sending the tree, attracted by a cycle’s vertex $a$, to the tree attracted by the next vertex $a^2$ of the attracting cycle.

Definition. A vertex has rank $r$, if it is separated from the attracting cycle by $r$ edges.

Example. The vertices of the attracting cycle have rank zero.

Consider an attracting cycle of period $T$, formed by the vertices $\{a, a^2, a^4, \ldots, a^{2^{T-1}}\}$, the next vertex of the cycle being $a$. In this case the following periodicity relation holds

$$a^S = 1, \text{ where } S = 2^T - 1.$$ 

Definition. The connection of the component of the graph attracted by a cycle of period $T$ is the map $P$ sending any vertex $b$ of rank $r$ to the vertex $Pb = b^x$, where $x = (2^r - 1)S + 2$ $r$ being the rank of $b$.

Example. For the vertices $(a, b_1, b_2, \ldots)$ of ranks $(0, 1, 2, \ldots)$ we have $Pa = a^2$, $ Pb_1 = b_1^{S+2}$, $ Pb_2 = b_2^{3S+2}$, $ \ldots$.

The periodicity condition $a^S = 1$ implies the conditions $b_1^{2S} = 1$, $b_2^{4S} = 1$, $\ldots$, $b_r^{2^rS} = 1$ for the vertices $b_r$ of rank $r$, since $b_r^{2^r} = a$ belongs to the attracting cycle.

The choice of $x(r)$ in the definition of connection is explained by the following lemma.

Lemma 1. The connection is a morphism of the monad:

$$P(b^2) = (P(b))^2.$$

Proof. The rank of $b^2$ is $r - 1$ for a vertex $b$ of rank $r$. Hence the following identities hold:

$$P(b^2) = (b^2)^y = b^{3y}, \quad y = (2^{r-1} - 1)S + 2;$$

$$(P(b))^2 = (b^x)^2 = b^{2x}, \quad x = (2^r - 1)S + 2.$$ 

The ratio of the two last expressions is equal to $b^{2(x-y)}$. But $2(x - y) = 2^rS$, hence the ratio is 1, and the lemma is thus proved.

Lemma 2. If two different vertices $b$ and $b'$ have the same square $b^2 = (b')^2$ then the vertices $c = b^x$ and $c' = (b')^x$ are also different.

Proof. Indeed the number $x$ is odd for $r > 0$. Denote it by $2k + 1$. Then the following identities hold

$$c = b(b^2)^k, \quad c' = b'(b^2)^k,$$

whence the equality $c = c'$ implies $b = b'$, proving the lemma.

Lemma 3. For a vertex $b$ of rank 1 the vertex $c = Pb$ can’t belong to the attracting cycle (and hence $c$ has rank 1).
Proof. If the vertex \( c = b^{s+2} \) were belonging to the attracting cycle, it would be a power \( a^{2^i} \) of the cycle vertex \( a = b^2 \). There are \( T \) such powers, but the equalities

\[
(Pb)^2 = P(b^2) = P(a) = a^2
\]

would imply that \( Pb = a \), i.e. \( b^{s+2} = b^2 \). The equality \( b^{s+2} = b^2 \) would imply \( b^{2^t+1} = b^2 \), whence the following equations would hold

\[
b = b^{2^t} = a^{2^{t-1}},
\]

and the rank of \( b \) would be 0 and not 1.

Lemma 4. The connection sends the tree attracted by the vertex \( a \) of the cycle, isomorphically onto the tree attracted by the next vertex: \( a^2 \) (preserving in particular the rank of the vertices).

Proof. Let \( n_i \) be the number of vertices of the tree attracted by the vertex \( a_i \) of the attracting cycle \( \{a_0 = a, a_1 = a^2, \ldots, a_i = a^{2^i}, \ldots\} \), \( (i = 0, 1, \ldots, T - 1) \). The isomorphisms into the next trees, discussed in Lemmas 1-3, imply the sequence of inequalities

\[
n_0 \leq n_1 \leq \ldots \leq n_T.
\]

The \( T \)-periodicity of the cycle implies that \( n_T = n_0 \), implying the equality of all numbers of the periodic sequence \( n_i \), and hence the isomorphisms of all the \( T \) attracted trees, proving the lemma (and hence Theorem 4).

Definition. The iterated connecting mapping \( M = P^T \), sending the tree attracted by any vertex of the attracting cycle isomorphically onto itself, is the monodromy (of the component of period \( T \)).

The monodromy acts identically on the lowest floors of the trees \( (r \leq 1) \), but might be non-trivial at the higher floors. It might be an interesting invariant of the group.

Example. For a cycle of period \( T = 5 \) and a vertex \( b \) of rank \( r = 2 \) the vertex \( b^4 = a \) belongs to the attracting cycle, whence \( a^{32} = a, a^{31} = 1, b^{124} = 1 \). In this case \( S = 31, x = 3S + 2 = 95, Mb = b^2, \) and \( z = 95^5 = 63 \mod 124 \). The point \( Mb = b^{63} \) might differ from \( b \), while their projections to the first floor of the tree \(-b^2\) and \((Mb)^2\) coincide: \( b^2 = b^{126} \).

7 Modular topology of Keplerian cubes

The graph of the squaring monad of the group \( G = SL(2, \mathbb{Z}_5) \) (consisting of 120 elements) has 17 components:

\[
[\text{graph}(G)] = T + 10A_2 + 6A_4.
\]

The rooted tree \( T \) has 32 vertices containing the point \( \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \), at the first floor and 30 points \( c \) of period 4 \( (c^4 = 1) \) at the second floor: \( r(T) = (1, 1, 30) \), counting the root 1 at the floor 0.
The periods of the points belonging to the $A_4$ components are equal to 5 (at the attracting cycles) and to 10 at the (only) first floors of the trees. Typical examples of this are the element \((1 \ 1) \ 1 \ 2\), of period 10 and its square \((2 \ 3) \ 3 \ 0\), of period 5.

The periods of the points belonging to the $A_2$ components are equal to 3 (at the attracting cycles) and to 6 at the (only) first floors of the trees. Typical examples of this are the element \((1 \ 1) \ 4 \ 0\), of period 6 and its square \((0 \ 1) \ 4 \ 4\), of period 3.

**Theorem 5.** The group $G = SL(2, \mathbb{Z}_5)$ acts on the projective line $\mathbb{P} = P^1(\mathbb{Z}_5)$ as a group of 60 even permutations of its 6 points.

To describe these permutations, consider the dodecahedron with its 12 pentagonal faces. Connect each face to the opposite one by a straight line, joining their centers.

The group of symmetries of the dodecahedron permutes these 6 lines.

To describe these 60 special even permutations (forming a small part of the total number 360 = $6!/2$ of even permutations of 6 elements), one should use Kepler’s construction (invented by him in his “Harmonia Mundi” to describe the lengths of the large axis of the planetary orbits of the Solar System in terms of the regular polyhedral nests).

Kepler inscribed 5 cubes into the dodecahedron. The edges of the 5 Keplerian cubes are the 60 diagonals of the 12 pentagonal faces of the dodecahedron. To choose one of the cubes, one should start from one of the diagonals of a face.

The 60 special permutations of 6 elements, produced by the action of the group $SL(2, \mathbb{Z}_5)$ on the finite projective line $\mathbb{P}$, are realized by the 60 rotations of the dodecahedron, forming its rotation group. They define all the 60 even permutations of the 5 Keplerian cubes. Thus the projective group of the finite projective line $\mathbb{P}$ (consisting of 6 points) is isomorphic to the group $S^+(5)$ of the even permutations of 5 elements (namely, of the 5 Keplerian cubes):

$$ (G = SL(2, \mathbb{Z}_5))/\{\pm 1\} \simeq S^+(5). $$

**Remark 2.** The group $G$ consists of 120 elements, as does the group $S(5)$ of permutations of 5 points. But these two groups of 120 elements are not isomorphic. Indeed, the matrix group $G$ has the center $\{\pm 1\}$ of two elements, while in the group of permutations the center is trivial.

**Remark 3.** The group $G$ is not the direct product $K \times H$, where the group $K = \{\pm 1\}$ consists of 2 elements.

Indeed, denote by $(R_0 = 1, R_1, R_2, \ldots)$ the ranks of the tree $T$ of the component of the graph of the group $H$, which contains the identity element of $H$.

The ranks of the product $A_1 \ast T$ are then $(1, 2R_1 + 1, 2R_2, \ldots)$, since the ranks of the graph $A_1$ of $K$ are $(1, 1)$ (we use the formula of the ranks of the product).

For the group $G$ the ranks of the tree containing the identity element are $(1, 1, 30)$. Hence if $G$ were isomorphic to $K \times H$, one would have $2R_1 + 1 = 1$, $2R_2 = 30$, whence $R_1 = 0,$
$R_2 = 15$, which is impossible, since the second floor is void when the first one is, while 15 is not equal to 0.

A similar reasoning proves also the non-triviality of the fibration $G \to G/K$ for $G = SL(2, \mathbb{Z}_p)$, $p > 5$.

In terms of the permutations of the finite projective line, the components of the graph of the squaring monad for the group $G = SL(2, \mathbb{Z}_5)$ can be described by the Young diagrams of the special even permutations of the Keplerian cubes, namely

$$A_1 \sim (5), \quad A_2 \sim (3 + 1 + 1), \quad T_r \sim (1 + 1 + 1 + 1 + 1)$$

at floors $r = 0$ and $r = 1$,

$$T_2 \sim (2 + 2 + 1) \quad \text{at floor 2}.$$

Geometrically a component of type $A_4$ is represented by the 4 non-trivial rotations of the dodecahedron, preserving its face (and hence preserving the opposite face). There are 6 such pairs of faces, 6 components, and hence 24 such non-trivial rotations.

The rotations produced by a component of type $A_2$ preserve a vertex of the dodecahedron (and hence preserve the opposite vertex). There are 10 such pairs of vertices, 10 such components, and hence 20 such non-trivial rotations of the dodecahedron.

The rotation representing an element of the second floor $T_2$, preserves an edge (and hence preserves the opposite edge). There are 15 such pairs of edges, 15 such elements, and together with the identity mapping (realized by the floors $T_0$ and $T_1$) we get all the $24 + 20 + 15 + 1 = 60$ rotations of the dodecahedron.

Consider similarly the group $G = SL(2, \mathbb{Z}_p)$, where $p$ is odd. It permutes the $p + 1$ points of the finite projective line $\mathbb{P} = P^1(\mathbb{Z}_p)$.

**Theorem 6.** These permutations are always even.

Indeed the generators $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ of $G$ have odd order $p$ in $G$ ($g^p = h^p = 1$). It follows that the representing permutations are even, since for an odd permutation $f$ its odd iteration $f^p$ is an odd permutation and so is different from the identity trivial permutation.

Thus the resulting group $G/\{\pm 1\}$ of special (projective) permutations of $p + 1$ points (consisting of some $p(p^2 - 1)/2$ even permutations) is much smaller than the whole group of the $(p + 1)!/2$ even permutations of $p + 1$ points.

The simplest example is the case $p = 7$, where the projective group $G/\{\pm 1\}$ contains 168 special even permutations of the 8 points of the finite projective line $\mathbb{P}$.

The dodecahedron should perhaps be replaced in this example by the “regular polyhedron” of genus $g = 3$, consisting of 24 faces (of 7 edges each one), meeting by 3 faces at 56 vertices, having 84 edges.

This polyhedron is associated to the singularity of the holomorphic $K_{12}$ function $x^2 + y^3 + z^7$ and to the Lobachevski triangle’s reflection group (for the angles $\pi/2$, $\pi/3$, $\pi/7$).
The peculiar combinatorics of the special permutations preserving the finite projective line structure, deserves a detailed study.

The required projective structure of the set of $p + 1$ points is fixed by a choice of the cyclic order in a fixed subset of $p - 1$ points. The subset is irrelevant but one should fix it to get the bijection between the cyclic orders and the projective structures.

For $p = 5$ there are 6 such structures, since there are 6 cyclic orders in a set of $p - 1 = 4$ elements $((m-1)! = (p-2)!$ cyclic orders of $m = p-1$ elements). Each of these 6 structures is preserved by the $360/6 = 60$ special permutations of the 6 points, associated to this structure.

For $p = 7$ there are $(p - 2)! = 5! = 120$ cyclic orders on a fixed subset of $p - 1 = 6$ points of the $p + 1 = 8$ points of the set $\mathbb{P}$. Any of these 120 structures is preserved by 

$$\frac{(p+1)!/2}{(p-2)!} = \frac{p(p^2-1)}{2} = 168$$

special even permutations of the $p + 1 = 8$ points of the finite projective line $\mathbb{P}$.

To generalize the Keplerian cubes permutations interpretation of the projective group $G/\{\pm 1\}$, one needs a combinatoric or geometric description of the permuted objects, generalizing the Keplerian cubes. It seems that the generalized dodecahedron vertices are the elements of order 3 of the group, and the group acts on the generalized dodecahedron by the conjugations.

8 Keplerian cubes and Hamiltonian subgroups

The classical Hamilton group consists of the 8 quaternionic unities $\{\pm 1, \pm i, \pm j, \pm k\}$. It is isomorphic to the connected component of the unity for the squaring monad of the group $SL(2, \mathbb{Z}_3)$ (which is the only group $SL(2, \mathbb{Z}_n)$ whose unity’s component of the squaring monad forms a subgroup).

The Keplerian cubes inscribed into the dodecahedron, and their $K_{12}$-generalisations are related to the subgroups of the unity’s component of the squaring monads of the groups $G = SL(2, \mathbb{Z}_p)$, isomorphic to the classical Hamilton group.

Among the 30 elements of order 4 at the second floor $T_2$ of the unity’s component of the squaring monad of $SL(2, \mathbb{Z}_5)$, there are 5 disjoint sextets, each forming together with the two elements 1 and -1 of floors 0 and 1 of $G = SL(2, \mathbb{Z}_5)$, a subgroup which is isomorphic to the classical Hamilton group.

All these 5 Hamilton subgroups of $G$ are conjugated in $G$.

To recognize the sextet one can use the relations $\{r^2 = -1, s^2 = -1, t^2 = -1\}$, verified by its two anti-commuting generators $r, s$ (having the product $t = rs$). To prove the statements on the sextets, formulated above, it is sufficient to consider one example, like the sextet $\{\pm r, \pm s, \pm t\}$, where
and to calculate the conjugations, preserving it. There are 12 such conjugations generated automorphisms. The 120 elements of $G$ act as 60 conjugation operations, since $axa^{-1} = -ax(-a)^{-1}$. The 60 conjugations of the chosen sextet provide 60/12 = 5 different sextets (and hence 5 different Hamilton subgroups in $G$), which are all conjugated to each other.

The product of two 4-th order elements of $G$ is an element of order 4 (verifying $(rs)^2 = 1$) exactly for those pairs $(r, s)$, which generate Hamilton subgroups. In particular, the elements of such a pair anti-commute (which is also useful to recognize them, since these are the only anti-commuting pairs of the 4-th order elements).

In the following table we present only 3 elements of each one of the 5 sextets $I - V$ (the other 3 being $-r$, $-s$, $-t$):

<table>
<thead>
<tr>
<th>sextet</th>
<th>$I$</th>
<th>$II$</th>
<th>$III$</th>
<th>$IV$</th>
<th>$V$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r$</td>
<td>$\begin{pmatrix} 0 &amp; 1 \ 4 &amp; 0 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 0 &amp; 2 \ 2 &amp; 0 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 2 &amp; 0 \ 0 &amp; 3 \end{pmatrix}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$s$</td>
<td>$\begin{pmatrix} 0 &amp; 2 \ 2 &amp; 0 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 0 &amp; 2 \ 2 &amp; 0 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 0 &amp; 2 \ 2 &amp; 0 \end{pmatrix}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t = rs$</td>
<td>$\begin{pmatrix} 2 &amp; 0 \ 0 &amp; 3 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 0 &amp; 3 \ 0 &amp; 3 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 0 &amp; 3 \ 0 &amp; 3 \end{pmatrix}$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table: The generators of the Hamilton subgroups of $SL(2, \mathbb{Z}_5)$.

The 5 Keplerian cubes are generated by these 5 Hamilton subgroups $H$ in the following way (imitating a formula for the matrix $A^h$, $h \in H$).

Consider a third order element $A$ of $G$. The conjugation by $A$ transforms any Hamilton subgroup of $G$ into a Hamilton subgroup. For a given Hamilton subgroup $H$ of $G$ there are 8 third order elements $A$, preserving the subgroup by $A$-conjugation:

$$AHA^{-1} = H.$$ 

These 8 third order elements are the 8 vertices of the Keplerian cube, associated to this Hamilton subgroup $H$.

These five cubes are presented in the next table by the quadruples $(a, b, c, d)$ of their vertices, the other four vertices of the cube being the inverse elements, $(a^2, b^2, c^2, d^2)$, of $G$:

<table>
<thead>
<tr>
<th>sextet</th>
<th>$I$</th>
<th>$II$</th>
<th>$III$</th>
<th>$IV$</th>
<th>$V$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$\begin{pmatrix} 1 &amp; 2 \ 3 &amp; 1 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 4 &amp; 4 \ 1 &amp; 1 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 4 &amp; 4 \ 1 &amp; 1 \end{pmatrix}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$b$</td>
<td>$\begin{pmatrix} 3 &amp; 2 \ 1 &amp; 1 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 2 &amp; 4 \ 3 &amp; 4 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 2 &amp; 4 \ 3 &amp; 4 \end{pmatrix}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$c$</td>
<td>$\begin{pmatrix} 3 &amp; 3 \ 1 &amp; 1 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 3 &amp; 3 \ 1 &amp; 1 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 3 &amp; 3 \ 1 &amp; 1 \end{pmatrix}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$d$</td>
<td>$\begin{pmatrix} 1 &amp; 4 \ 3 &amp; 3 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 3 &amp; 3 \ 1 &amp; 1 \end{pmatrix}$</td>
<td>$\begin{pmatrix} 3 &amp; 3 \ 1 &amp; 1 \end{pmatrix}$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table: The Keplerian cubes of the dodecahedral surface of $SL(2, \mathbb{Z}_5)$. 

21
Each of the 10 vertices appears in the table twice, and there are exactly 2 Keplerian cubes, containing each vertex. The table contains (taking the squares into account) all the 20 third order elements of \(G\), each of them appearing twice (belonging to two cubes).

The vertices of the Keplerian cubes can be easily calculated, using the following properties of these elements of \(G\).

Orient the cube and its faces, and let \(P, Q, R, S\) be the sequence of the vertices of a face (ordered accordingly to the face orientation). Then \(PQ = QR = RS = SP\) is the associated element of the sextet of the Hamilton group, the same for the 4 edges. The association of the 6 sextet’s elements to the 6 faces of the cube has the following defining property: the product of the three elements, associated to the three faces, meeting at a cube vertex, is always equal to 1 (there are 12 such colorings of the cube’s faces by the sextet’s elements, the cube’s rotations transforming one of these colorings to all the others).

A different characterization of the same relation between the Hamilton group and the Keplerian cube states: four vertices of the cube are obtained from one of them (say, \(A\)), conjugating it by the 8 elements of the Hamilton group: \(\{A, rAr^{-1}, sAs^{-1}, tAt^{-1}\} \) (\(-r\) acting as \(r\)).

The 4 opposite vertices of the Keplerian cube are the inverse third order elements of the group \(G\), that is \(\{A^2, rA^2r^{-1}, \ldots\}\).

The edges of the cube are connecting the vertices (numbered at the figure by the Hamilton group elements) in the following way, shown in the figure:

![Figure 5: The cubical pattern of the Hamilton group.](image)

The preceding constructions interpolate the associations \(1 \mapsto A, -1 \mapsto A^{-1}\), attributing some “values” to \(A^r\) and similarly at the others cube vertices.

In terms of the dodecahedron surface, the Keplerian cubes edges are the diagonals of the faces.

The dodecahedron surface had been constructed combinatorially from the group \(G\), using at its vertices the 3-d order elements of the group, while the surface’s faces had been defined by a choice of one from the two conjugacy classes of elements of order 5 in \(PSL(2, \mathbb{Z}_5)\) (or of order 10 in \(G = SL(2, \mathbb{Z}_5)\)). There are, accordingly two “dodecahedral” surfaces with the same vertices, but with different faces and edges (similarly to the regular pentagon and to its inscribed pentagonal star in the plane).
The corresponding Keplerian cubes, formed by the faces diagonals, have the same vertices for both dodecahedral surfaces, as it follows from the vertices description, given above in terms of the group $G$, where the dodecahedral surface had not been used.

However the edges lists and their relations to the faces diagonals are different on the two “dodecahedral” surfaces. These two surfaces are sent (together with their cubes edges) one to the other by a $GL(2, \mathbb{Z}_5)$-conjugation, generated by a matrix, whose determinant is not a quadratic residue, say by $\left( \begin{array}{cc} 2 & 0 \\ 0 & 1 \end{array} \right)$.

9 The heptagon’s surfaces and their Keplerian cubes

It seems that the preceding theory might be extended to many other groups, for instance to other groups $G = SL(2, \mathbb{Z}_p)$. In the case $p = 7$ one obtains the following results.

**Theorem 7.** There are exactly 14 Hamilton subgroups in the part $T_0 + T_1 + T_2$ of the tree of the squaring monad of $G$. All these Hamilton subgroups are conjugated to one of the two of them, which two are not conjugated one to the other in $G$ (being conjugated in the larger group $G = GL(2, \mathbb{Z}_7)$).

The generators $(r, s)$ of these 14 Hamilton subgroups and the products $t = rs$ are presented in the following table (for the 7 groups, all conjugated to each other):

<table>
<thead>
<tr>
<th>group</th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
<th>V</th>
<th>VI</th>
<th>VII</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r$</td>
<td>$\left( \begin{array}{cc} 0 &amp; 1 \ 6 &amp; 0 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 2 &amp; 4 \ 4 &amp; 5 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 3 &amp; 2 \ 2 &amp; 4 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 0 &amp; 2 \ 3 &amp; 0 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 0 &amp; 3 \ 2 &amp; 0 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 1 &amp; 6 \ 2 &amp; 6 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 1 &amp; 3 \ 4 &amp; 6 \end{array} \right)$</td>
</tr>
<tr>
<td>$s$</td>
<td>$\left( \begin{array}{cc} 2 &amp; 3 \ 3 &amp; 5 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 1 &amp; 5 \ 1 &amp; 6 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 3 &amp; 4 \ 1 &amp; 4 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 2 &amp; 6 \ 5 &amp; 5 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 2 &amp; 5 \ 6 &amp; 5 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 1 &amp; 4 \ 3 &amp; 6 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 1 &amp; 2 \ 6 &amp; 6 \end{array} \right)$</td>
</tr>
<tr>
<td>$t$</td>
<td>$\left( \begin{array}{cc} 3 &amp; 5 \ 5 &amp; 4 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 6 &amp; 6 \ 2 &amp; 1 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 4 &amp; 6 \ 3 &amp; 3 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 3 &amp; 3 \ 6 &amp; 4 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 4 &amp; 1 \ 4 &amp; 3 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 5 &amp; 5 \ 6 &amp; 2 \end{array} \right)$</td>
<td>$\left( \begin{array}{cc} 5 &amp; 6 \ 5 &amp; 2 \end{array} \right)$</td>
</tr>
</tbody>
</table>

Table: Hamilton subgroups of $SL(2, \mathbb{Z}_7)$.

The others 7 Hamilton subgroups, which are not conjugated to these 7, are obtainable from this table by the group automorphism

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}
\]

(the Hamilton subgroup $\tilde{I}$, dual to $I$, being generated by $\left( \begin{array}{cc} 0 & 8 \\ 1 & 6 \end{array} \right)$, $\left( \begin{array}{cc} 2 & 4 \\ 3 & 2 \end{array} \right)$ and so on).

The 14 sextets of these 14 Hamilton subgroups provide $6 \cdot 14 = 84$ elements of order 4, while the second floor $T_2$ of the monad of $G$ contains only 42 elements.

The resulting intersections of the sextets are related to the 4 colors problem by the following construction.

Consider the graph, whose 14 vertices are the 14 Hamilton subgroups of $G$, and whose edges connect the vertices, whose sextets do intersect. The resulting graph can be described as a subset of the two dimensional torus, subdividing it into 7 hexagons, meeting by 3 at the 14 vertices. Each hexagon has a common edge with anyone of the others (see the figure.
below), and hence the resulting 7 countries map on the torus can not be colored regularly with less than 7 colors. The 7 subgroups, conjugated to $A$, are shown by the small circles at the figure below.

This covering of the torus by 7 hexagons can be obtained from a regular hexagon in the Euclidean plane $\mathbb{R}^2$. The union of the hexagon surface with its six mirrors reflections in its 6 sides covers a plane polygon, which is a fundamental domain of a translation group $\mathbb{Z}^2$, preserving the plane decomposition into congruent hexagons. The quotient torus $T^2 = \mathbb{R}^2 / \mathbb{Z}^2$ is subdivided into 7 hexagons, as it is shown in the figure (where $\mathbb{Z}^2$ is generated by $AA'$, $AA''$).

![Diagram of the torus covering by 7 hexagons]

Figure 6: The intersections pattern of the 14 Hamilton subgroups of $SL(2, \mathbb{Z}_7)$.

The isomorphism of the intersections pattern of the 14 sextets with this torical graph is verified by direct (but long) calculations of the 84 matrices $\{\pm r, \pm s, \pm t\}$.

The construction of the Keplerian cubes from the 14 Hamilton subgroups repeats the $SL(2, \mathbb{Z}_5)$ case construction, described above, and provides the 14 “Keplerian” cubes, of which 7 are conjugated to one of them, and 7 to another. The conjugations act on each cube as its rotations group.

The cubes can be shown on the generalized dodecahedral surface $M$ (covered by 24 hexagons, meeting along 84 edges, forming a genus 3 surface with 56 vertices, at each of which there meet three faces). The vertices are the elements of order 3 of $G$, and the faces are defined by the order 14 elements $c = ab$, $c^7 = -1$, $a^3 = b^3 = 1$.

To save paper, I had only constructed the quotient surface, obtained from the following folding of $M$ (see Figure 7).

The mapping, sending each matrix $A$ to the transposed inverse matrix $\tilde{A}$, is a group automorphism of $G = SL(2, \mathbb{Z}_7)$ (conjugating by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$). It acts on the third order elements, sending each of them to a third order element, and hence acts on the vertices set of our surface $M$, generalizing the dodecahedron.
Figure 7: The fundamental domain of the torical surface $M' = M/(\sim)$. 
It sends the 14-th order element of $G$, used to define the surface, to a conjugated 14-th order element, and hence sends the edges of the surface to the edges, preserving the cyclical order of three edges at a common vertex, acting on $M$, preserving the patterns, defined above.

Thus we can define the quotient surface $M'$ and the quotient patterns, the folding $M \rightarrow M'$ being the identification of any $A$ with $\tilde{A}$.

The surface $M'$ has only 28 vertices and only 12 heptagonal faces, and their pattern is less complicated, than the one of the whole 24-faced surface $M$. Drawing everything on $M'$, it is not difficult to reconstruct the covering pattern on $M$.

The mapping $M \rightarrow M'$ is in fact a two-fold ramified covering with four ramification points, topologically equivalent at each of them to the $\sqrt{z}$ complex ramification. The ramification points are not the vertices of the structure defined above, but rather the middle points of some edges.

The 56 vertices of the surface $M$, associated to the group $G = SL(2, \mathbb{Z}_7)$, are the 28 matrices $\begin{pmatrix} i \end{pmatrix}$, and the 28 matrices $\begin{pmatrix} i \end{pmatrix} = \begin{pmatrix} i \end{pmatrix}^2$, $(1 \leq i \leq 13$ and $15 \leq i \leq 29)$, the 28 matrices $\begin{pmatrix} i \end{pmatrix}$ being listed in the following table:

<table>
<thead>
<tr>
<th>$i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>18</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>18</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>18</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>18</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$i$</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>29</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>16</td>
<td>15</td>
<td>16</td>
<td>15</td>
<td>16</td>
<td>15</td>
<td>16</td>
<td>15</td>
<td>16</td>
<td>15</td>
<td>16</td>
<td>15</td>
</tr>
</tbody>
</table>

Table: Third order elements of the group $SL(2, \mathbb{Z}_7)$.

The 12 heptagonal faces of the surface $M'$ are shown in the figure together with the names of their neighbours, and the quotient torical surface $M'$ is the result of the identifications $A \sim \tilde{A}$ along the bold line bounding the fundamental domain, consisting of 12 heptagonal areas.

The 4 ramification points of the covering $M \rightarrow M'$ are the middle points of the boundary segments $(A\tilde{A})$, which 4 segments are $(3, 11)$ in the area $XI$, $(23, 22)$ in the area $I$, $(6, 9)$ in the area $XII$ and $(15, \tilde{I}6)$ in the area $V$.

The complex structures of the surfaces $M$ and $M'$ would be specially interesting, since the resulting elliptic curve structure on $M'$ might be used to relate the $SL(2, \mathbb{Z}_7)$ algebra to the geometry and arithmetics of elliptic functions.
\ln(\text{sum}(N(n))) vs \ln(n)
References


