2003

I hope the problems of the list below might be useful even for beginners, being however open and allowing both experimental discoveries of new facts and creation of general theories.

2003-1. Fermat–Euler statistics and number-theoretic turbulence. Consider the sequence $\{a^t\}$, $t = 1, 2, \dots$, of residues $\bmod n$ (where the integers a and n are relatively prime, $(a, n) = 1$). Fermat and Euler proved that this sequence is periodic. Denote by $T(n, a)$ its (minimal) period such that $a^T \equiv 1 \pmod{n}$. It behaves very irregularly.

Examples: $T(509, 2) = 508$, $T(511, 2) = 9$.

Billions of experiments (mostly by F. Aicardi) showed that *the average growth rate of* $T(n)$ (as $n \to \infty$) *is asymptotically* $Cn/\log n$. For smaller values of n, the slower growth rate $Cn^{7/8}$ was observed.

The problem is to prove (or disprove) this asymptotic behavior (at least for $a = 2$, n being odd).

The words "average growth rate of $A(n)$ is asymptotically equal to $B(n)$" mean that

$$\lim_{n\to\infty} \frac{\sum_{k=1}^{n} A(k)}{\sum_{k=1}^{n} B(k)} = 1.$$

One also says in this case that *B is the Cesàro asymptotic of A*.

Example: The Cesàro asymptotic of $\sin^2(\pi n/2)$ is $1/2$.

A discussion of this problem can be found in the article: ARNOLD V. I. Topology and statistics of formulae of arithmetics. *Russian Math. Surveys*, 2003, **58**(4), 637–664. This article also contains a discussion of the relation of the study of this average growth to the discovery of turbulence laws by Kolmogorov: his methods were used in Aicardi's work.

2003-2. Randomness of arithmetic progressions. Consider the sequence $\{at\}$, $t = 1, 2, \dots, T$, of residues $\bmod n$ (a and n being relatively prime, $(a, n) = 1$). The problem is to study the statistics of the distribution of this sequence of T elements in the finite circle $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ of residues $\bmod n$.

As a randomness characteristic of a set of T points of the finite circle of n points, we consider the sum of the squares of the lengths of the T arcs into which the circle is divided by T chosen points,

$$R = \sum_{i=1}^{T} a_i^2, \quad \sum a_i = n.$$

To avoid the influence of the scale n, we consider the reduced dimensionless number

$$r = \frac{R}{n^2}, \quad \frac{1}{T} \leq r \leq 1.$$

To eliminate the influence of the parameter T, we reduce the randomness characteristic once more, dividing r by its minimal value:

$$s = \frac{r}{r_{\min}} = Tr, \quad 1 \leq s \leq T.$$

These characteristics were introduced and studied in the article quoted in problem *2003-1*.

Example: The minimal value $s_0 = 1$ of the binormalized randomness parameter s is attained by the choice of the T vertices of a regular T-gon (an army line distribution of points at equal distances). The maximal value $s_1 = T$ corresponds to the degenerate choice of a cluster of T points at the same place.

The random choice (of independent uniformly distributed points in a circle) leads to the "freedom-liking" value $s_* = 2T/(T+1)$ of the birandomness parameter, which is close to 2 when there are many points.

Measuring the value of s for a given set, one can evaluate some kind of degree of its randomness. Namely, the observation $s < s_*$ is a sign of some mutual repulsion of points of the set (reaching the minimal value $s_0 = 1$ of the parameter s for maximal repulsion, leading to an army line formation).

Similarly, the observation of larger values of the binormalized randomness parameter, $s > s_*$, is a sign of some mutual attraction of points of the set (reaching the maximal value of the parameter $s = T$ for the strongest attraction, leading to a cluster formation).

Intermediate values of the binormalized randomness parameter s (close to s_*) are a sign of independence of the T points of the set which is, in this case, "more random" than in the cases of repulsion or attraction.

It is interesting to compare the values of the binormalized randomness parameter s for different sets of residues $\bmod n$. The experiments with the full periods T of geometric progressions of residues, discussed above in problem *2003-1*, have shown mostly some repulsion ($s \approx 1.5$), but no theorem on such a repulsion is known.

Problem *2003-2* is *to study* (at least experimentally) *the values of the binormalized randomness parameter s for the T points of the arithmetic progression* $\{at\}$*,* $t = 1, 2, \ldots, T$*, of residues modulo n* (*integers a and n being relatively prime*).

Remark: One may predict a significant difference in the answers depending on the choice of the length T of the progression, at least in the following two cases.

1) One may choose T randomly, say between 1 and $n/2$, and study the distribution of the values $s(n, a, T)$ for large values of n and random independent choices of a and T.

2) One may choose $T(n, a)$ to be one of the denominators of the continued fraction approximation of the number

$$\frac{a}{n} = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cdots}} = [x_0, x_1, x_2, \ldots].$$

The approximation is provided by the truncated continued fraction

$$\frac{p_k}{q_k} = [x_0, x_1, \ldots, x_k],$$

and the proposal is to choose $T = q_k$ (for some randomly chosen k).

One might conjecture that there is more repulsion and army line structure in the second case, but there are yet no theorems confirming it, and it would be interesting to verify this conjecture by numerical experiments.

One proposal is to calculate $s(n, a, k)$ for all the continued fraction k-approximations of all the fractions a/n, $1 \leq n \leq N$, trying to guess the behavior of the distribution of the values of s for $N \to \infty$.

One might also try to suggest the natural science conjectures on these behaviors (in both cases 1) and 2)), using the Gauss–Kuz′min distribution of the elements x_i of the continued fractions of random real numbers. It would be difficult to deduce the behavior of s from this distribution in a rigorous way; therefore I suggest rather a semi-empirical study in which one uses such intuitively probable things as the independence of different prime numbers with no proof (which might rely on deep number theory involving the Riemann zeta function conjecture).

Nonrigorous deductions freely using these unproved properties of number theory sometimes would become correct proofs many years later (as it happened to Legendre's discovery of the distribution of prime numbers proved only by Hadamard and Vallée Poussin).

Continuing with numerical experiments, one might also study many other sequences of residues of, say, (T subsequent prime numbers) mod$(n = 100)$. The choice $n = 100$ facilitates finding these residues in the tables of primes.

For the theory of continued fractions, one might see, for instance, the book ARNOLD V. I. Continued Fractions. Moscow: Moscow Center for Continuous Mathematical Education Press, 2001, 40 pp. (in Russian).

One might try to apply the Gauss–Kuz′min statistics of continued fractions to the study of geometric progressions of residues, for example, $\{2^t \pmod{n}\}$, reducing it to the arithmetic progression of logarithms $\{t \ln 2\}$ and investigating their distribution in the "random" intervals $\big(\ln n + \ln k; \ln n + \ln(k+1)\big)$ of lengths $b = \ln((k+1)/k) \approx 1/k$.

Supposing the randomness of the real number $(\ln 2)/b$ and applying its continued fraction statistics, one might come to some (empirical) conjectures on the distributions of elements of arithmetic progressions of logarithms in the above "random" interval of length b (for random k). The properties of these distributions might be interpreted (while exponentiating) as those of the distributions of the residues $\{2^t \pmod{n}\}$ (which should then be compared with the numerically observed properties).

The proofs of the "randomness" properties conjectured for these studies might be much more difficult than their fearless applications, which might immediately lead to the conjectures to be verified numerically (ignoring missing foundations, such as "randomness" proofs, which might appear centuries later, as happened to the Legendre statistics of the prime numbers distribution).

2003-3. Modular groups and their Kepler cubes. Consider the group $G = \mathrm{SL}(2, \mathbb{Z}_p)$ consisting of the matrices of order 2, whose elements are residues mod p and determinant is equal to 1. This group consists of $p(p^2-1)$ matrices.

We associate with a finite group a directed graph (called its *monad*), whose vertices are elements of the group and arrows lead just from each element to its square (one arrow leaving each vertex).

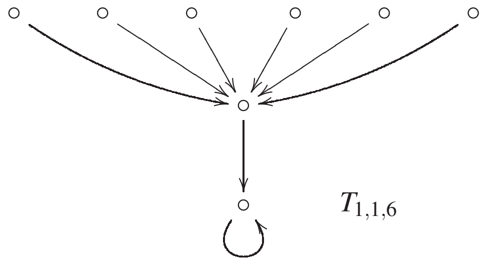
Example: The monad of the cyclic group $\mathbb{Z}_4$ of order 4 is

$$\begin{tikzcd}
1 \arrow[dr] & & \\
& 2 \arrow[r] & 0 \arrow[loop right] \\
3 \arrow[ur] & &
\end{tikzcd}$$

(denoting the elements additively as the residues mod 4).

Problem: Find the monad of the group $G = \mathrm{SL}(2, \mathbb{Z}_p)$ (for any prime number p).

Example: For $p = 3$, the monad $[G]$ consists of five components: one rooted tree $T_{1,1,6}$ and four components A_2.



$T_{1,1,6}$

A_2

Each A_2-graph is a cycle of length 2 with trees of length 1 attached to its vertices. The T-component is a subgroup isomorphic to the group $\{\pm 1, \pm i, \pm j, \pm k\}$ of quaternionic units.

For $p = 5$, the monad $[G]$ consists of 17 components: one rooted tree with 32 vertices, 10 components A_2, and 6 components A_4 (the directed graph A_m being a cycle of length m with trees of length 1 attached to each of its vertices, thus having in all $2m$ vertices):

$$[G] = T_{1,1,30} \sqcup (10A_2) \sqcup (6A_4).$$

The 5 *Kepler cubes* are inscribed in a dodecahedron. The vertices of any Kepler cube are some 8 of the 20 vertices of the dodecahedron. The 12 edges of any Kepler cube are 12 diagonals of the 12 pentagonal faces of the dodecahedron (one diagonal of each face).

The group $G = \mathrm{SL}(2, \mathbb{Z}_5)$ contains 5 "Hamilton subgroups" isomorphic to the Hamilton group of the eight quaternionic units $\{\pm 1, \pm i, \pm j, \pm k\}$. These subgroups lie in the tree $T_{1,1,30}$ of the monad. Each Hamilton subgroup consists of the lower floor elements 1, -1 of the tree and of six elements of order 4 lying on the highest floor. These 5 disjoint sextuples cover all 30 elements of the highest floor of the tree.

The vertices of the dodecahedron associated with G are the 20 third order elements of G (forming the cycles of the 10 components A_2 of the monad). The pentagonal faces of the dodecahedron correspond to the 5th (and 10th) order elements of G (forming the A_4-components of the monad).

The 5 Kepler cubes are related to the 5 Hamilton subgroups in the following way. Fix a Hamilton subgroup. Consider the subgroup of G formed by the elements such that, conjugating G by these elements, one transforms the chosen Hamilton subgroup into itself. This isotropy subgroup contains 24 elements: the 8 elements of the Hamilton subgroup, 8 elements of order 3, being the vertices of the Kepler cube associated with the chosen Hamilton subgroup, and 8 elements of order 6, forming an opposite cube (whose matrices are obtained from the Kepler cube matrices, multiplying them by -1). All vertices of the Kepler cubes belong to the ten A_2-components of the monad.

The vertices of any Kepler cube are obtained from one of them, conjugating it by the elements of the corresponding Hamilton subgroup. These 8 conjugations provide 4 of the 8 vertices of the cube; the other 4 are the inverses of these (or their squares, since all elements of the Kepler cube are of order 3).

One may say that the preceding construction interprets the mysterious informal expression of the Kepler cube vertices in terms of one of them, A, as being the 8 matrices A^h, $h \in \{\pm 1, \pm i, \pm j, \pm k\}$. Namely, $h = 1$ and $h = -1$ provide A and A^{-1}, while the meaning of A^i and of the others is explained by the above construction of conjugations generating the Kepler cube from the corresponding Hamilton subgroup.

Let us return to the part of the problem devoted to p-Kepler cubes. It requires *to extend the theory of Kepler cubes of the group* $G = \mathrm{SL}(2, \mathbb{Z}_5)$ *described above, replacing* 5 *by a larger prime number* p.

One of the first results in this direction is the following study of tree complexity. Consider a chain of k consecutive squarings,

$$A_0, \quad A_1 = A_0^2, \quad A_2 = A_1^2, \quad \dots, \quad A_k = A_{k-1}^2 = 1.$$

It is represented in the monad as a chain

$$A_0 \to A_1 \to A_2 \to \cdots \to A_k = 1$$

of length k (containing $k+1$ elements of the group).

Theorem: A nondegenerate chain of length k in $G = \mathrm{SL}(2, \mathbb{Z}_p)$ exists if and only if $p \equiv \pm 1 \pmod{2^k}$.

The nondegeneracy means the absence of the matrix 1 (except at the last place): $A_{k-1} \neq 1$, $A_k = 1$.

Example: Chains with $k = 2$ exist for $p = 5, 11, 13$. Chains with $k = 4$ exist for $p = 17, 47$.

Perhaps, these chains of squarings provide the generalizations of Kepler cubes to the case $p > 5$.

The combinatorics of some generalized Kepler cubes for $p = 7$ is described in the article ARNOLD V. I. Topology and statistics of formulae of arithmetics. *Russian Math. Surveys*, 2003, **58**(4), 637–664. This article also explains the relation of the combinatorics of these cubes to the generalized four-color problem on a toroidal surface and to some Riemannian surfaces associated with the monad of G.

The *Riemannian surface of the monad of* G is constructed as a complex of dimension 2, whose vertices are the third order elements of G, but a relevant interpretation of complex structure in terms of combinatorial group theory of G is still missing.

It would also be interesting to extend this study of monads and Riemannian surfaces to the case of *complex versions of finite modular groups*, $G_{\mathbb{C}} = \mathrm{SL}(2, \mathbb{CZ}_p)$, where $\mathbb{CZ}_p$ is the ring of complex integers modulo p:

$$\mathbb{CZ}_p = \{a + bi : a \in \mathbb{Z}_p,\ b \in \mathbb{Z}_p\}.$$

2003-4. Matrix version of Fermat's small theorem. This recent theorem asserts the congruence of traces:

$$(\mathrm{tr} A)^p - \mathrm{tr}(A^p) = pF;$$

here p is a prime number, A is any unimodular matrix of integers, $A \in \mathrm{SL}(n, \mathbb{Z})$, the ratio F (the result of the division of the difference by p) being a polynomial in the variables $\sigma_1, \dots, \sigma_p$ with integer coefficients, where σ_i are the coefficients of the characteristic polynomial of A at the terms of degree $\leq p$:

$$\sigma_1 = \sum_i \lambda_i, \quad \sigma_2 = \sum_{i<j} \lambda_i \lambda_j, \quad \dots, \quad \sigma_p.$$

An equivalent statement is the formula

$$(\lambda_1 + \dots + \lambda_n)^p - (\lambda_1^p + \dots + \lambda_n^p) = pF(\sigma_1(\lambda), \dots, \sigma_p(\lambda)).$$

The proofs are available in the paper: ARNOLD V. I. Matrix Fermat theorem, finite circles and finite Lobachevsky plane. *Funct. Anal. Appl.*, 2004, **38**(1), 20 pp.

Example 1: The "cube of the sum" formula

$$(a+b)^3 - (a^3 + b^3) = 3(a+b)ab$$

can be extended to the identity

$$(a + b + \dots + z)^3 - (a^3 + b^3 + \dots + z^3) = 3(UV - W),$$

where $U = \sigma_1 = a + \dots + z$, $V = \sigma_2 = ab + \dots + yz$, $W = \sigma_3 = abc + \dots + xyz$.

Example 2: For the identity matrix $A = 1$ of order n, our congruence takes the form

$$n^p - n = pF,$$

implying Fermat's small theorem: $n^{p-1} \equiv 1 \ (p)$ if $(n, p) = 1$.

The Newton polynomials F with integer coefficients have (in the cases $p \leq 7$ for which I have explicitly calculated them) rather small coefficients, mostly equal to ± 1 (neglecting the 0 coefficients implied by the weighted homogeneity of the polynomial F, the weight of its variable σ_i being equal to i). Another rather curious property of these coefficients is the equilibrium between the numbers of positive and negative coefficients ($+UV$ and $-W$ above) whose total sum is 0 for $p > 2$.

The present problem is *to develop the theory of these strange polynomials F and to generalize the traces congruence to other symmetric functions, for instance, to the congruences for the other coefficients of the characteristic polynomial of the power* A^p (or, in a matrix-free formulation, to other Tschirnhausen transformations).

The *Euler extension of Fermat's small theorem*, replacing the prime p by any integer m and replacing the Fermat congruence $a^{p-1} \equiv 1 \ (p)$ by the Euler congruence $a^m \equiv a^{m-\varphi(m)} \ (m)$, might also have *matrix versions*, which would be interesting even as conjectures guessed from calculating many examples. The simplest example in this direction replaces the prime p by any integer m and the difference $(a+b)^p - (a^p + b^p)$ by $\sum C_m^k a^k b^{m-k}$, the integer k in the sum being relatively prime with m: $(k,m) = 1$. The claim is the set of the congruences: C_m^k is divisible by m, C_{m-1}^{k-1} is divisible by k (provided that $(k,m) = 1$).

Example: For $m = 9$, the binomial coefficients $C_9^k = \mathbf{1}, 9, 36, \mathbf{84}, 126, 126, \mathbf{84}, 36, 9, 1$ are divisible by 9 if $k \neq 0, 3, 6, 9$.

For $k = 3$, the binomial coefficients $C_{m-1}^2 = \mathbf{1}, 3, 6, \mathbf{10}, 15, 21, \mathbf{28}, 36, \dots$ are divisible by 3 if $m \neq 3, 6, 9, \dots$

Proof of the congruences $C_m^k \equiv 0 \ (m)$ and $C_{m-1}^{k-1} \equiv 0 \ (k)$: Consider a subset X of k elements in the set $\mathbb{Z}_m$ of residues $\bmod m$. The translations $t_a : x \mapsto x + a$ $(a = 1, \dots, m)$ move X into other subsets of k elements, which are all different if $(k,m) = 1$, since otherwise we would obtain a bijection t_a of X to itself whose period T would be a common divisor of m and k. Thus we get a free action t_a of the group $\mathbb{Z}_m$ on the set of its subsets X of k elements, whose number C_m^k is therefore divisible by m.

The divisibility of C_{m-1}^{k-1} by k follows, since $C_m^k = \frac{m}{k} C_{m-1}^{k-1}$ and $(k,m) = 1$.

The question is therefore *to generalize these results from the binomial case to the multinomial coefficients of* $(a + \cdots + z)^m$.

Among recent peculiar discoveries in this direction, we note the strange degree $x(a,b)$ of the prime p, to whose power the difference of binomial coefficients is divisible,

$$C_{pa}^{pb} - C_a^b = p^{x(a,b)} z \quad \text{(where } (p,z) = 1).$$

It seems (empirically) that x is an averagely growing function, but its asymptotic behavior is known only empirically, showing also the strange (and unproved) independence of the values $x(p^m + 1, b)$ (and sometimes of $x(pm + 1, b)$) of the value b of the second argument.

Example: For $p=3$, the starting values of the degree $x(a,b)$ form a Pascal-type triangle (the rows $a=2,3,\ldots,7$ being shown, $b=1,\ldots,a-1$ in each row a):

$$
\begin{array}{c}
2\\
4 \quad 4\\
3 \quad 3 \quad 3\\
2 \quad 3 \quad 3 \quad 2\\
4 \quad 4 \quad 5 \quad 4 \quad 4\\
3 \quad 3 \quad 3 \quad 3 \quad 3 \quad 3
\end{array}
$$

For $p=5$, the rows ($a=2,3,\ldots,11$) of the values $x(a,b)$ are:

$$
\begin{array}{c}
3\\
3 \quad 3\\
3 \quad 3 \quad 3\\
5 \quad 5 \quad 5 \quad 5\\
4 \quad 4 \quad 4 \quad 4 \quad 4\\
3 \quad 4 \quad 4 \quad 4 \quad 4 \quad 3\\
3 \quad 3 \quad 4 \quad 4 \quad 4 \quad 3 \quad 3\\
3 \quad 3 \quad 3 \quad 4 \quad 4 \quad 3 \quad 3 \quad 3\\
5 \quad 5 \quad 5 \quad 5 \quad 6 \quad 5 \quad 5 \quad 5 \quad 5\\
4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4
\end{array}
$$

The double periodicity,

$$x(a+p,b)=x(a,b)=x(a+p,b+p),$$

observed in this table, is partially preserved for other prime numbers p.

For $p=7$, the rows ($a=2,3,\ldots,15$) of the values $x(a,b)$ are:

$$
\begin{array}{c}
3\\
3 \quad 3\\
3 \quad 3 \quad 3\\
3 \quad 3 \quad 3 \quad 3\\
3 \quad 3 \quad 3 \quad 3 \quad 3\\
5 \quad 5 \quad 5 \quad 5 \quad 5 \quad 5\\
4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4\\
3 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 3\\
3 \quad 3 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 3 \quad 3\\
3 \quad 3 \quad 3 \quad 4 \quad 4 \quad 4 \quad 4 \quad 3 \quad 3 \quad 3\\
3 \quad 3 \quad 3 \quad 3 \quad 4 \quad 4 \quad 4 \quad 3 \quad 3 \quad 3 \quad 3\\
3 \quad 3 \quad 3 \quad 3 \quad 3 \quad 4 \quad 4 \quad 3 \quad 3 \quad 3 \quad 3 \quad 3\\
5 \quad 5 \quad 5 \quad 5 \quad 5 \quad 5 \quad 6 \quad 5 \quad 5 \quad 5 \quad 5 \quad 5 \quad 5\\
4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \quad 4
\end{array}
$$

The functions $x(mp^r+1,b)$ of m and r are rather peculiar, and I leave to the reader the pleasure of finding them, thus continuing, at least empirically, the Fermat experimental way of discovery of mathematical facts (see the tables below).

All these facts can be extended from the binomial coefficients to the multinomial ones, as well as to the coefficients K of the Newton–Girard formula (taking into account that, for $p=2$, one should replace the difference $C_{pa}^{pb}-C_a^b$ by the twisted difference $C_{pa}^{pb}-(-1)^b C_a^b$).

The table of the first values of $x(p^r+1,b)$ (independent of b) is:

$r \backslash p$	2	3	5	7	9	11	13	17	19	23
1	2	3	4	4	4	4	4	4	4	4
2	3	4	5	5	5	5	5	5	5	5
3	4	5	6	6	6	6	6	6	6	6
4	5	6	7	7	7	7	7	7	7	7
5	6	7	8	8	8	8	8	8	8	8
6	7	8	9	9	9	9	9	9	9	9
7	8	9	10	10	10	10	10	10	10	10
8	9	10	11	11	11	11	11	11	11	11
9	10	11	12	12	12	12	12	12	12	12

We see that $x(p^r+1,b)=r+3$ for $p>3$ (being $r+2$ for $p=3$ and $r+1$ for $p=2$), but this is proved only by some millions of examples.

The tables of the first values of $x(mp^r+1,b)$ (independent of b) are given and discussed below (for $p=3,5,7,11$).

Case $p=3$:

$m \backslash r$	1	2	3	4	5	6	7	8	9	10
1	3	4	5	6	7	8	9	10	11	12
2	3	4	5	6	7	8	9	10	11	12
3	4	5	6	7	8	9	10	11	12	13
4	3	4	5	6	7	8	9	10	11	12
5	3	4	5	6	7	8	9	10	11	12
6	4	5	6	7	8	9	10	11	12	13
7	3	4	5	6	7	8	9	10	11	12
8	3	4	5	6	7	8	9	10	11	12
9	5	6	7	8	9	10	11	12	13	14
10	3	4	5	6	7	8	9	10	11	12
11	3	4	5	6	7	8	9	10	11	12
12	4	5	6	7	8	9	10	11	12	13
13	3	4	5	6	7	8	9	10	11	12
14	3	4	5	6	7	8	9	10	11	12
15	4	5	6	7	8	9	10	11	12	13

Case $p = 5$:

$m \backslash r$	1	2	3	4	5	6	7	8	9	10
1–4, 6–9, 11–14	4	5	6	7	8	9	10	11	12	13
5, 10, 15	5	6	7	8	9	10	11	12	13	14

Case $p = 7$:

$m \backslash r$	1	2	3	4	5	6	7	8	9	10
1–6, 8–13, 15	4	5	6	7	8	9	10	11	12	13
7, 14	5	6	7	8	9	10	11	12	13	14

Case $p = 11$:

$m \backslash r$	1	2	3	4	5	6	7	8	9	10
1–10, 12–15	4	5	6	7	8	9	10	11	12	13
11	5	6	7	8	9	10	11	12	13	14

One sees that $x(mp^r + 1, b) = r + 3$ for $(m, p) = 1$, $p \geq 3$.
Here is the table of the function $y(a, b)$ defined by the twisted difference

$$C_{2a}^{2b} - (-1)^b C_a^b = 2^{y(a,b)} z, \quad (2, z) = 1$$

(the rows correspond to $a = 2, 3, \ldots, 20$, $1 \leq b < a$):

3
1 2
5 6 5
1 3 2 3
3 5 4 5 3
1 2 1 3 1 2
7 8 7 9 7 8 7
1 4 3 4 2 4 3 4
3 6 5 6 4 6 5 6 3
1 2 1 4 2 3 2 4 1 2
5 6 5 8 6 7 6 8 5 6 5
1 3 2 3 1 4 3 4 1 3 2 3
3 5 4 5 3 6 5 6 3 5 4 5 3
1 2 1 3 1 2 1 4 1 2 1 3 1 2
9 10 9 11 9 10 9 12 9 10 9 11 9 10 9
1 5 4 5 3 5 4 5 2 5 4 5 3 5 4 5
3 7 6 7 5 7 6 7 4 7 6 7 5 7 6 7 3
1 2 1 5 3 4 3 5 2 3 2 5 3 4 3 5 1 2
5 6 5 9 7 8 7 9 5 7 6 9 7 8 7 9 5 6 5

The apparent "double periodicity" of this function would relate to $y(a,b)$ the values $y(a+8,b)$ and $y(a+8,b+8)$, but $y(16,1)=9\neq 7=y(8,1)$.

It is, for instance, formally unknown whether the values $x(a,b)$ are bounded or unbounded (neither for a fixed prime p nor totally) and whether the small values (like 2) appear finitely or infinitely many times. Such questions are also open for the multinomial coefficients (where, sometimes, the answers might be different and the results might be easier than for the particular case of binomial coefficients).

2003-5. Weak asymptotics of Frobenius numbers. The *Frobenius number* $K(a_1,\dots,a_s)$, defined by s integers a_i having no common divisor altogether, is the least integer which, together with all greater integers, belong to the additive semigroup A of integers generated by the summands a_i:

$$A=\{k_1a_1+\dots+k_sa_s : k_i\geq 0,\ k_i\in\mathbb{Z}\}.$$

Example: For $s=2$, $a_1=3$, $a_2=5$ the semigroup is

$$A=\{0,3,5,6,8,9,10,\dots\},$$

hence the Frobenius number is $K(3,5)=8$.

The Frobenius number of two (relatively prime) numbers was calculated by J. J. Sylvester: $K(a,b)=(a-1)(b-1)$ (*Educational Times*, 1884, **41**, p. 21).

The problem is to find the asymptotic behavior of the very irregular function $K(a)$ of $s>2$ variables for large vectors $a\in\mathbb{Z}^s$.

The conjectural averaged behavior is

$$K\sim C\cdot\sqrt[s-1]{\prod a_i},\quad C=\sqrt[s-1]{(s-1)!}$$

(for instance, $K(a,b,c)\sim\sqrt{2abc}$).

The averaging means the following construction (or its generalization). Let us replace the vector a by a neighborhood U of radius r of the scaled vector $Na\in\mathbb{Z}^s$. Now replace the value $K(a)$ by the (arithmetic) mean $\widehat{K}_N$ of the values $K(b)$ of Frobenius number at the points b of the neighborhood U whose components b_i have no common divisor greater than 1.

The conjecture is that, *for growing values of N, the mean values $\widehat{K}_N$ have a limit* (*probably provided by the conjectured formula above*): $\lim\limits_{N\to\infty}\widehat{K}_N$ *should grow as* const $\cdot\left(\prod a_i\right)^{1/(s-1)}$ *for large a.*

I have fixed above the averaging radius r, but one might also choose some growth rate $r(N)$, where $r(N)/N$ tends to 0 when N tends to infinity.

More on the weak asymptotic behavior is provided in the article: Arnold V. I. Weak asymptotics for the numbers of solutions of Diophantine problems. *Funct. Anal. Appl.*, 1999, **33**(4), 292–293. Applications of Frobenius numbers to representation theory are discussed in the article: Arnold V. I. Frequent representations. *Moscow Math. J.*, 2003, **3**(4), 14 pp.

2003-6. Frequent representations. Consider a unitary representation of a finite group in Hermitian space $\mathbb{C}^N$. The representation is called *frequent*, if the dimension of the variety of those representations in the same space, which are unitary equivalent to the given one, has the maximal possible value.

I have proved that *the multiplicities of irreducible summands in a frequent representation of a finite group are asymptotically proportional to their dimensions when N tends to infinity*.

The problem is *to find similar asymptotic proportions for orthogonal* (*and quaternionic*) *representations of finite groups*.

One might also try to extend the result to the case of *infinite groups*, taking into account the decomposition of the *regular representation* in the space of functions on the group (which contains, for a finite group, each irreducible component as many times as its dimension).

Regular representations might be decomposed into irreducible ones in the case of an infinite group too, and one might try *to replace sums by infinite series* (in the discrete case) or by *integrals* (in the case of compact Lie groups).

As an intermediate problem in this direction, one might study *the asymptotic behavior of the multiplicities of irreducible representations in the spectrum of the Laplace operator on such groups as* $\mathrm{SO}(3)$ *or* $\mathbb{S}^3 = \mathrm{Spin}(3) = \mathrm{SU}(2)$.

The rotated eigenfunction remains an eigenfunction (with the same eigenvalue), and therefore the function space is decomposed as the orthogonal sum of spaces of irreducible representations, corresponding to different eigenvalues.

Considering the first M eigenvalues, one obtains a set of multiplicities of irreducible components, and the problem is *to find the behavior of the ratios of these multiplicities for M tending to infinity*.

In the case of a finite symmetry group, this proportion seems to be asymptotically the same as in a frequent representation (I observed it for millions of eigenfunctions, studying quasimodes in 1972 and working in magnetohydrodynamics in the 1980s). This *choice of frequent representations* (made by Nature, arranging the eigenfunctions symmetry) *seems to take place for any elliptic system with a* (*finite*) *symmetry, say, for the Laplace operators on compact Riemannian manifolds having a symmetry group such as the ordinary ellipsoids*.

However, some attempts of my students (to whom I had shown this phenomenon discovered by me in many examples) to prove it as a general theorem were not very successful, and therefore I repeat here *the natural representation frequency conjecture for eigenfunctions of symmetric systems* as a problem to work on (even in the case of finite groups and unitary representations where it is simpler).

The first examples of frequent representations are published in the article: ARNOLD V. I. Modes and quasimodes. *Funct. Anal. Appl.*, 1972, **6**(2), 94–101; *the Russian original is reprinted in*: Vladimir Igorevich Arnold. Selecta–60. Moscow: PHASIS, 1997, 189–202.

Magnetohydrodynamical applications (*to the Sakharov–Zeldovich fast dynamo problem*) are published in the paper: ARNOLD V. I. Evolution of a magnetic field under the action of drift and diffusion. In: Some Problems in Modern Analysis. To the memory of V. M. Alexeev. Editor: V. M. Tikhomirov. Moscow: Moscow University Press, 1984, 8–21 (in Russian). See also the survey article: ARNOLD V. I. Remarks on the perturbation theory for Mathieu type problems. *Russian Math. Surveys*, 1983, **38**(4), 215–233.

The dimensions of the spaces of eigenfunctions considered numerically in these studies reached many millions, the symmetry group being that of the cube in the magnetohydrodynamical paper.

A recent study of frequent unitary representations, providing the proof of the asymptotic proportion of irreducible components for the case of finite groups is published in the article: ARNOLD V. I. Frequent representations. *Moscow Math. J.*, 2003, **3**(4), 14 pp.

2003-7. Symmetric group representations and asymptotic statistics of Young diagrams. Irreducible representations of the finite symmetric group $S(n)$ are labeled (by Frobenius) by their Young diagrams of area n, representing the *partitions*

$$n = a_1 + \cdots + a_s$$

of the parameter n into natural summands. One usually orders the summands, supposing that $a_1 \geq a_2 \geq \cdots \geq a_s$, representing a partition by its *Young diagram* D consisting of n unit squares in the plane. The first (longest) row consists of a_1 squares filling the rectangle

$$0 \leq x \leq a_1, \quad -1 \leq y \leq 0.$$

The next row (below the first one) consists of a_2 squares filling the rectangle

$$0 \leq x \leq a_2, \quad -2 \leq y \leq -1,$$

and so on, up to the last (shortest) row filling the rectangle

$$0 \leq x \leq a_s, \quad -s \leq y \leq -s+1.$$

The corresponding unitary irreducible representation lies in the Hermitian space $\mathbb{C}^{a(D)}$, its dimension $a(D)$ being equal to the number of *monotonic fillings* of the n squares of the diagram D by n numbers $\{1, \ldots, n\}$. A filling is monotonic if these numbers are decreasing along rows and columns of the diagram (that is, while x or $-y$ are growing in our notation).

Example: The partition $5 = 3 + 2$ provides 5 monotonic fillings

$$\begin{pmatrix} 5 & 4 & 3 \\ 2 & 1 & \end{pmatrix}, \quad \begin{pmatrix} 5 & 4 & 2 \\ 3 & 1 & \end{pmatrix}, \quad \begin{pmatrix} 5 & 4 & 1 \\ 3 & 2 & \end{pmatrix}, \quad \begin{pmatrix} 5 & 3 & 2 \\ 4 & 1 & \end{pmatrix}, \quad \begin{pmatrix} 5 & 3 & 1 \\ 4 & 2 & \end{pmatrix},$$

therefore $a(3+2)=5$. The maximal value of the dimension of the representation is attained at the partition $5=3+1+1$ and is equal to 6.

Vershik and Kerov proved a remarkable property of the *maximal dimension* value $\overline{a}(n)$ (of the dimensions $a(D)$ of the representations corresponding to all Young diagrams D of area n):

Theorem: *The asymptotic behavior of the maximal dimension value $\overline{a}(n)$ for $n \to \infty$ coincides with that of the average dimension value, taking the averaging along all Young diagrams D of area n weighted with weights w proportional to the squares of the dimensions of representations, $w(D) \sim a^2(D)$.*

This theorem on the coincidence of the maximum with the average implies that there exist a lot of Young diagrams D for which the dimension $a(D)$ is very close to the maximal value $\overline{a}(n)$.

The problem is *to evaluate the number of Young diagrams D of area n for which*

$$a(D) > \overline{a}(n) - C$$

(*at least asymptotically for large n, at least averaging in n, and eventually with some dependence of C on n, for instance, counting the diagrams D satisfying the condition $a(D) > \overline{a}(n)(1-c_1)$*).

The goal of these studies is to apply them to understanding the asymptotic behavior of decompositions of frequent representations into irreducible ones, for which one also needs to study, using the Frobenius numbers, the semigroup generated by the dimensions of irreducible representations (see problem *2003-5*).

The Vershik–Kerov theorem is proved in the article: VERSHIK A. M., KEROV S. V. Asymptotics of maximal and typical dimensions of irreducible representations of a symmetric group. *Funct. Anal. Appl.*, 1985, **19**(1), 21–31.

A more or less classical *explicit formula for generalized Catalan numbers $a(D)$* is proved, for instance, in the article: ARNOLD V. I. Frequent representations. *Moscow Math. J.*, 2003, **3**(4), 14 pp. Its strange proof is based on singularity theory (and on the Euler–Jacobi complex residue formula asserting the vanishing of the sum of the inverse values of the Jacobian of a mapping $\mathbb{C}^r \to \mathbb{C}^r$ over all preimages of a generic point).

The answer is

$$a(D) = \frac{n!}{h_1!\cdots h_n!}\prod_{i<j}(h_i - h_j),$$

where $h_i = a_i + s - i$ are the lengths of "hooks."

Most results of the study of symmetric groups admit natural extensions to *all Coxeter groups* (at least to the 4 classical series A_k, B_k, C_k, D_k, but in many cases to other crystallographic groups E_6, E_7, E_8, F_4, G_2 and even to noncrystallographic ones $I_2(p)$, H_3, H_4).

Unfortunately, neither the Vershik–Kerov theorem quoted above nor other remarkable results of Vershik's theory on the asymptotic statistics of representations of symmetric groups were extended to the case of other Coxeter groups. See, for instance, the recent survey book: Asymptotic Combinatorics with Applications to Mathematical Physics (St. Petersburg, 2001). Editor: A. M. Vershik. Berlin: Springer, 2003 (Lecture Notes in Math., 1815).

I propose therefore as a problem the suggestion to find *conjectural forms of these extensions* (at least for the 4 classical series A, B, C, D). Such an extension might provide a better understanding of the results which are already known for the classical series A of symmetric groups.

For instance, Vershik discovered that *a typical Young diagram of large area n, being observed from a distant location, looks in most cases like a standard universal curvilinear astroidal triangle*

$$\{(x,y) : f(x)+f(y) \leq 1,\ x \geq 0,\ y \geq 0\}$$

for some special function f (explicitly calculated by him) *growing from* $f(0)=0$ *to* $f(1)=1$.

Namely, the image of the Young diagram under some motion and homothety (reducing its area n to the constant area of universal astroidal triangle) almost coincides with this triangular domain, the difference being small for large n.

Here the *majority* (of "*typical*" Young diagrams) is understood in the sense of weighting, whose weights $w(D)$ are proportional to $a^2(D)$, as in the Vershik–Kerov theorem.

The problem is to find universal domains of this type for other Coxeter groups (or complex simple Lie algebras).

2003-8. Elliptic integrals and functions, their topological nonelementarity and topological Galois theory. The fact that elliptic functions and elliptic integrals do not belong to the set of elementary functions is well known. The problem is to prove that this event has a topological nature: *they are not topologically equivalent to any elementary function*.

I proved in 1963 the corresponding version of the Abel theorem on the unsolvability of algebraic equations of degree 5 (or higher). These equations (for instance, the equation $x^5+ax+1=0$) are topologically unsolvable in radicals: no one (complex) function, topologically equivalent to the algebraic 5-valued function $x(a)$, is a finite combination of radicals and univalent functions (for instance, rational functions).

The topological proof of this *topological unsolvability* theorem (based on the topological complexity of the monodromy group and on the topology of Riemannian surfaces) was proved in my lectures of 1964 for Moscow high school students (which started with the definitions of complex numbers, fundamental groups and Riemannian surfaces). Notes of these lectures were later published by one of the students as the book: ALEXEEV V. B. Abel's Theorem in Problems. Moscow: Nauka, 1976 (in Russian); *the French translation*: Cassini, to appear.

In my lectures, I attributed these topological results to Abel, mentioning also his parallel results on topological unsolvability of differential equations and on topological nonelementarity of integrals (proved by the topological complexity of the branchings of the corresponding multivalued complex functions).

However, my students, trying to find the exact statements and proofs in Abel's works, never discovered them, and thus *the problem of proving the topological nonelementarity of elliptic integrals and functions remains open*.

An elliptic integral is sampled by, for instance, the time function for the Newton equation with cubic potential,

$$t(X) = \int_0^X \frac{dx}{\sqrt{f(x)}}, \quad f(x) = x^3 + ax + b$$

(say, for $a = 1$, $b = 0$).

The claim is that *this multivalued function of X is not topologically equivalent to any elementary function* (which is a finite combination of rational functions, radicals, exponential or logarithmic functions, trigonometric or inverse trigonometric functions), and that this remains true even if one also allows any univalent functions in combination.

An elliptic function is a meromorphic doubly periodic function, such as the Weierstrass $\wp$-function $\wp = X(t)$ (inverse to the preceding elliptic integral).

My 1963 conjecture (attributed by me to Abel) claims that *this function is also topologically nonequivalent to any elementary function* (*and that this remains true even if one extends the class of elementary functions by adding combinations with any univalent functions of a finite number of variables*).

Both statements (on elliptic integrals and elliptic functions) are different, and I am unable to reduce one of them to the other.

My 1963 reasoning provides a topological proof of the nonelementary character of the dependence of the periods of integrals on parameters (such as a and b above). Namely, the (modular) monodromy group of this multivalued function is not possible for any elementary function (and hence for any function topologically equivalent to an elementary one).

I would also mention a project of an (ugly) proof of the topological nonelementarity of an elliptic function. Suppose that $\wp$ is reduced to an elementary function f by a homeomorphism h (so that $f(x) = \wp(h(z))$). Then one should prove that h must be holomorphic (since f and $\wp$ are). Next, one should deduce from the Riemann classification of holomorphic simply connected domains that h should be an affine transformation, and therefore that f is an elliptic function (whenever it is topologically equivalent to such a function). The final step is to use the well known fact of the nonelementarity of the elliptic function $\wp$ itself (whose ugly proof ought to be replaced by a topological one, still missing).

To study the left-right topological nonequivalence of elliptic functions to elementary ones, one should first prove that an action of the group $\mathbb{Z}^2$ on a complex plane domain by holomorphic diffeomorphisms, which is topologically equivalent to the standard action by the translations, is in fact holomorphically equivalent to an (eventually different) action by some translations.

Such a reasoning forces any meromorphic function, which is topologically left-right equivalent to an elliptic function, to be genuinely elliptic (and hence nonelementary).

Similarly, for an algebraic mapping $a: X \to Y$ between closed Riemannian surfaces, one should try to prove that any perturbed holomorphic mapping belongs to the same family of algebraic mappings $\tilde{a}: \tilde{X} \to \tilde{Y}$.

Applying this algebraicity result to the "automorphic mapping" $f: G \to Y$, $f = a \circ \pi$ ($\pi: G \to X$ being a covering), one hopes to deduce the automorphic character of the perturbed meromorphic mapping $\tilde{f}: \tilde{G} \to \tilde{Y}$, $\tilde{f} = \tilde{a} \circ \tilde{\pi}$, provided that it is left-right topologically equivalent to the nonperturbed automorphic mapping f.

On the other hand, one might suppose that the situation is different in higher dimensions and that the automorphic character of the nonperturbed mapping f might be disturbed by a perturbation $\tilde{f}$ preserving the left-right topological equivalence class of f, the perturbed mapping $\tilde{f}$ being no longer automorphic.

In 1964, I attributed the preceding theory to Abel, asking my students to publish the resulting "Topological Galois Theory" formally, but they have not succeeded yet.

2003-9. Cubic irrationals and tori triangulations related to higher-dimensional continued fractions. Consider a unimodular matrix with integer elements,

$$A \in G = \mathrm{SL}(n, \mathbb{Z}),$$

whose eigenvalues are different positive irrational numbers. The n eigenplanes divide the space $\mathbb{R}^n$ into 2^n ortants invariant under the action of A.

This action also preserves the integer lattice $\mathbb{Z}^n \subset \mathbb{R}^n$, and hence preserves its intersection with each ortant.

Each of these intersections is an additive semigroup of integer vectors. Its convex hull is bounded by an infinite polyhedral surface called the *sail*.

The sail is invariant under the action of A, but it is also invariant under the action of other linear mappings belonging to G and having the same eigenplanes (with positive eigenvalues). Such mappings form a commutative symmetry group H of the sail (isomorphic to $\mathbb{Z}^{n-1}$); I use to call it "the integer version of the Cartan subgroup," since its matrices are diagonal matrices with the same eigenbasis.

Now consider the quotient variety (the sail)$/H$. For $n = 2$, it is a circle divided into segments $s_1, \dots, s_k$, and each segment is equipped with the "integer points" (being the images of lattice points of the sail). Let s_i be decomposed by these integer points into a_i void arcs. Then the sail is associated with the periodic continued fraction with period $[a_1, \dots, a_k]$, equal to the number $\lambda = a_1 + 1/(a_2 + \dots + 1/(a_k + 1/\lambda) \cdots)$.

This number λ describes the eigendirection of the second order matrix A in suitable $\mathrm{SL}(2,\mathbb{Z})$-integer coordinates of $\mathbb{R}^2 \supset \mathbb{Z}^2$.

Similarly, for $n > 2$ we obtain a decomposition of a torus T^{n-1} into faces (which are the images of convex faces of the sail) and their intersections, each containing "integer points" (being the images of those of the sail). This structure is called "the $(n-1)$-dimensional periodic continued fraction" (of the initial operator $A \in G$).

The problem is to find out, *which "triangulations"* (decompositions into faces) *and which sets of "integer points" are possible for the matrices of order* 3, $A \in \mathrm{SL}(3,\mathbb{Z})$.

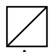
In the case of ordinary continued fractions ($n = 2$), any period $[a_1, \dots, a_k]$ is possible, but the situation becomes less clear already for cubic irrationals ($n = 3$).

Example: The golden ratio matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ has a natural extension to an arbitrary dimension n, which is the matrix

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

for $n = 3$ and similarly

$$A = \begin{pmatrix} n & n-1 & n-2 & \dots \\ n-1 & n-1 & n-2 & \dots \\ n-2 & n-2 & n-2 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

for any n. The corresponding triangulation (for $n = 3$) divides the 2-torus T^2 into 2 triangles represented by the decomposition of the square by a diagonal: . There are no integer points other than the four vertices of the square (representing a single point of the torus).

The problem involves three questions on these T^2-triangulations associated with cubic irrationals (being the eigenvalues of the characteristic polynomial of A).

1) *Which triangulations are possible* (first forgetting the integer points, but then taking them into account in the classification of triangulated structures)?

2) *Which triangulations are typical* (also either forgetting the integer points or taking them into account)?

For instance, consider all those matrices in G whose elements are not too large (say, $\|A\| \le R$) and eigenvalues are all positive.

Count the numbers of the triangles, quadruples, pentagons (and so on) of their triangulated structures. What is the asymptotics (for R tending to infinity) of the ratios of these numbers? Are there more triangles than quadrangles?

Similar statistics are interesting for the numbers of integer points (on faces and edges), for the number of faces meeting at a vertex, for integral lengths of edges, integral areas of faces, integral dihedral angles between the faces along an edge, integral solid angles at vertices, and so on.

Even without a study of asymptotics for $R \to \infty$ (which might, however, be easier than a detailed study for fixed R which is, say, less than 10), the tables of answers to the preceding questions on frequency might be interesting even for small values of R.

Later, one might compare these empirical tables with the universal statistics for the sails of arbitrary triangular pyramids described by Kontsevich and Sukhov, with no relation to integer matrices A: it would be interesting to see whether the proportions described above converge, as $R \to \infty$, to the proportions for random pyramids (whose existence and independence of a pyramid for almost all pyramids was proved by Kontsevich and Sukhov). Unfortunately, they present no values for these proportions (such as the ratio of the frequency of the triangular case to that of the quadrangular case), whose existence was proved in their article.

Details of these studies are described in the book: Pseudoperiodic Topology. Editors: V. Arnold, M. Kontsevich and A. Zorich. Providence, RI: Amer. Math. Soc., 1999 (AMS Transl., Ser. 2, 197; Adv. Math. Sci., 46).

The first study of periodic higher-dimensional continued fractions is published in the paper: TSUCHIHASHI H. Higher-dimensional analogues of periodic continued fractions and cusp singularities. *Tôhoku Math. J., Ser.* 2, 1983, **35**(4), 607–639.

The simplest triangulations of T^2 (into two triangles) were described by E. Korkina in: KORKINA E. I. Two-dimensional continued fractions. The simplest examples. *Proc. Steklov Inst. Math.*, 1995, **209**, 124–144.

More discussions of higher-dimensional continued fractions (and of their relations to many objects, such as the classification of graded commutative algebras and to the theory of Gröbner bases) are in the book ARNOLD V. I. Continued Fractions. Moscow: Moscow Center for Continuous Mathematical Education Press, 2001, 40 pp. (in Russian) ("Mathematical Education" Library, 14).

To the preceding questions on possible triangulations and frequent triangulations, I add the following question on equivalence:

3) *What are common features of those triangulations which correspond to isomorphic fields of algebraic numbers*?

Knowing a triangulation (equipped with the "integer points"), how to describe all the triangulations associated with matrices A having the same characteristic polynomial (or isomorphic fields of algebraic numbers)? Is the number of such "algebraically equivalent" triangulations finite (for a given initial triangulation)?

Anyway, the explicit calculation of algebraic invariants of the field, generated by the eigenvalues of A, in terms of the corresponding triangulation might be useful for many purposes, even if it does not answer the preceding equivalence question.

For instance, one might study the arising combinatorial invariants of sails also for the nonperiodic case, where the algebraic invariants of the periodic case might generate interesting ergodic geometry type asymptotics of the finite part of the sail combinatorics.

In the case of usual continuous fractions, the celebrated Lagrange theorem says that the periodicity of the continued fraction of a number is equivalent to the fact that it is a quadratic irrational number.

For the case of higher-dimensional continued fractions, the deduction of periodicity from algebraic origin (based on the Dirichlet theorem on the units) is provided in Tsuchihashi's article quoted above.

The inverse theorem is available at present only partially. In the article KORKINA E. I. La périodicité des fractions continues multidimensionnelles. *C. R. Acad. Sci. Paris, Sér.* I *Math.*, 1994, **319**(8), 777–780, some theorem, implying the deduction of the algebraic origin of a pyramid from the topological periodicity of a sail's structure, is announced, but, unfortunately, its complete proof is still missing.

I am mentioning this theorem here (trying also to urge the publication of the proof), since the derivation of the matrix A from the period of the sail's triangulation, leading to the proof of this theorem of Korkina, might help to understand which triangulated structures (on T^2) can be obtained from suitable matrices A of order 3.

The first steps and first numerical experiments in the direction of questions 1)–3) posed above were made by O. Karpenkov (Moscow State University, 2003). He mostly studied Sylvester matrices

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & a & b \end{pmatrix}$$

finding a lot of triangulations. He proved, however, that some of the relevant matrices cannot be reduced to any Sylvester form (it is unknown whether such matrices are exceptional or rather typical).

It is formally unknown neither whether the number of topologically nonequivalent triangulations of T^2, associated with the matrices corresponding to isomorphic cubic fields, is finite or infinite, nor whether the number of fields corresponding to isomorphic triangulations is finite or infinite.

Even the infiniteness of the total set of the triangulations classes associated to all the matrices of $\mathrm{SL}(3,\mathbb{Z})$ is (formally) unproved.

The triangulations that do not correspond to any such matrix are (formally) unknown: are they typical or exceptional?

It is also formally unknown which of the classification problems discussed above are algorithmically solvable, and which ones are not (even for the reducibility of the Frobenius form).

There is no published information on the (undoubtedly existing) correlations between the sails in different ortants, into which the 3 eigenplanes divide $\mathbb{R}^3$ (between the 2^{n-1} different sails in the 2^n ortants of $\mathbb{R}^n$, for $n > 2$).

Even if some of the questions formulated above happen to be not difficult, the subjects are so fundamental that the answers should be published.

2003-10. Extensions of Courant's theorem on the topological structure of eigenfunction nodes. Let u be an eigenfunction of the Laplace operator, $\Delta u = \lambda u$, on a connected compact manifold (eventually with a boundary and suitable boundary conditions).

The Courant theorem asserts that, ordering the eigenfunctions by decrease of eigenvalues (tending to $-\infty$), one has the following restriction on the topological structure for the n-th eigenfunction: *the number of connected components, into which the zeros hypersurface of the n-th component divides the manifold, is at most n*:

$$b_0(\{x : u_n(x) \neq 0\}) \leq n.$$

Problem: Extend this theorem to the case of systems of equations, describing oscillations of the sections of fibrations whose fiber has dimension $m > 1$.

In this case, the zeros set would be generically a submanifold of codimension m, and one might study the dependence of its homology or homotopy properties on the number n, ordering the eigenvalues, such as $b_1(\{x : u_n(x) \neq 0\}$ or π_1, for $m = 2$; this corresponds to H^{m-1} in the general case. The system of two equations

$$\Delta u = \lambda u, \quad \Delta v = \lambda v, \qquad \text{for } (u(x,y), v(x,y)),$$

is the simplest example where one might even try to imitate arguments from Courant's proof, connecting points of common zeros by curves along which the vectors $(u(x,y), v(x,y))$ are parallel, and replacing, in the domains bounded by these curves, the eigenvector (u, v) by its "reflected" version.

Similarly, one might consider the case of one independent variable and two dependent ones, trying to majorize, for a fixed number of the eigenvalue, the rotation number of the plane vector $(u(x), v(x))$ along the base circle $\{x \pmod{2\pi}\}$ (supposing the normal fibration of an oscillating circle to be trivial).

Similar homotopic questions occur every time when the dimension of the normal bundle (fiber) exceeds the dimension of the base (space of independent variables); in this case, the zeros set of the eigenvector is generically empty, but the homology or homotopy class of the spherical bundle section might be evaluated in terms of the number of the eigenvalue.

2003-11. Generalizations of gravitational and Coulomb fields. Consider the space of Hermitian matrices of order n as a real vector space $\mathbb{R}^N$ where $N = n^2$. We consider them as matrices of Hermitian operators in the Hermitian space $\mathbb{C}^n$.

Consider the subvariety $\Sigma \subset \mathbb{R}^N$ formed by the matrices having a multiple eigenvalue. The codimension of this real algebraic variety is equal to 3 (look at the case $n = 2$ where Σ is the set of real scalar matrices).

The complement of Σ in $\mathbb{R}^N$ is the base space of the n eigenvectors fibrations (we normalize the eigenvectors to have norm 1, making each fiber a circle $\mathbb{S}^1$): they are formed by the normalized eigenvectors of the base space operator.

These fibrations have natural “adiabatic connections,” transporting an eigenvector to the closest vector of the neighboring fiber (corresponding to a perturbed operator).

Take, for instance, the case $n = 2$ reducing the space $\mathbb{R}^4$ of Hermitian matrices to the space $\mathbb{R}^3$ of traceless ones. In this 3-space, the multiple spectrum variety Σ is reduced to one point (the origin), and the connection’s curvature is a closed 2-form in $\mathbb{R}^3 \setminus \Sigma$.

This 2-form might be interpreted as a divergence-free vector field (using the volume element in $\mathbb{R}^3$). This vector field is smooth in $\mathbb{R}^3$ outside the origin; at the origin, it has a singularity. The latter is a Newton or Coulomb type singularity: the vector is directed along the radius-vector and its length is inverse proportional to the squared distance to the origin.

The problem is to extend this field to the case of matrices of higher order n. Say, if $n = 3$ the space of traceless matrices is $\mathbb{R}^8$, and the variety of multiple spectrum operators Σ_2 in it is 5-dimensional. It contains a subvariety Σ_3 of the operators having triple eigenvalues, which is just the origin.

The cone Σ_2 can be described in terms of its intersection with the sphere $\mathbb{S}^7$, bounding a neighborhood of Σ_3. This 4-dimensional intersection consists of two components (defined by the equations $\lambda_1 = \lambda_2$ and $\lambda_2 = \lambda_3$ for the usual ordering $\lambda_1 \le \lambda_2 \le \lambda_3$ of the eigenvalues).

The three curvature 2-forms of the three eigenvectors fibrations define the product closed 6-form corresponding to a vector field. This field has Newton or Coulomb singularities along Σ_2, but it has a worse singularity at the triple spectrum variety Σ_3.

Hence we arrive at the problem: study these Σ_3-generalizations of Newton or Coulomb forces (as well as their higher-dimensional versions for $n > 3$ and their quaternionic versions associated with multiple spectra of hyper-Hermitian forms).

The study of stratification singularities of Hermitian forms started in the article ARNOLD V. I. Modes and quasimodes. *Funct. Anal. Appl.*, 1972, **6**(2), 94–101; *the Russian original is reprinted in*: Vladimir Igorevich Arnold. Selecta–60. Moscow: PHASIS, 1997, 189–202. More details are described in the articles: ARNOLD V. I. Remarks on eigenvalues and eigenvectors of Hermitian matrices, Berry phase, adiabatic connections and quantum Hall effect. *Selecta Math.* (*N. S.*), 1995, **1**(1), 1–19; *the Russian translation in*: Vladimir Igorevich Arnold. Selecta–60. Moscow: PHASIS, 1997, 583–604; ARNOLD V. I. Relatives of the quotient of the complex projective plane by complex conjugation. *Proc. Steklov Inst. Math.*, 1999, **224**, 46–56; ARNOLD V. I. Polymathematics: is mathematics a single science or a set of arts? In: Mathematics: Frontiers and Perspectives. Editors: V. I. Arnold, M. Atiyah, P. Lax and B. Mazur. Providence, RI: Amer. Math. Soc., 2000, 403–416; CEREMADE (UMR 7534), Université Paris-Dauphine, № 9911, 10/03/1999.

The suggestion to study Σ_3-generalized Newton or Coulomb vector fields originated from M. Berry, while he was discussing the results of the above paper in *Selecta Math.* with the author who had related the Radon adiabatic connection (1918) to the theories of Berry phase described by Rytov (1938) and Ishlinsky (1952): RYTOV S. M. Sur la transition de l'optique ondulatoire a l'optique geométrique. *C. R.* (*Dokl.*) *Acad. Sci. USSR* (*N. S.*), 1938, **18**(2), 263–266; ISHLINSKY A. YU. Mechanics of special gyroscopic systems. Kiev: Academy of Sciences of Ukrainian SSR, 1952 (in Russian); *reproduced in*: Orientations, Gyroscopes and Inertial Navigation. Moscow: Nauka, 1976, p. 195.

2003-12. Finite order projective line geometry. The finite projective line $\mathrm{P}(\mathbb{Z}_p)$ (p being a prime number) is formed by the one-dimensional subspaces of the 2-dimensional vector space $\mathbb{Z}_p^2$:

$$\mathrm{P}(\mathbb{Z}_p) = \frac{\mathbb{Z}_p^2 \setminus 0}{\mathbb{Z}_p \setminus 0}, \quad \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

It consists of $p+1$ points which can be denoted by an affine coordinate taking the values

$$x \in \{0, 1, \ldots, p-1; \infty\}.$$

The finite p-projective line P consists of $p+1$ points:

$$\mathrm{P}(\mathbb{Z}_p) = \mathbb{Z}_p \sqcup \{\infty\}.$$

It is decomposed here into the affine part and the completing point at infinity. This decomposition depends on the coordinate choice and is not included in the structure of the projective line.

The group of unimodular p-matrices of order 2,

$$G = \mathrm{SL}(2, \mathbb{Z}_p),$$

acts on $\mathrm{P}(\mathbb{Z}_p)$ permuting one-dimensional vector subspaces of the plane $\mathbb{Z}_p^2$. This action is naturally reduced to the action of the quotient projective group

$$\mathrm{P}G = \mathrm{PSL}(2, \mathbb{Z}_p) = G/\{\pm 1\},$$

which is half as large as G (having only $p(p^2-1)/2$ elements).

The permutations of the $p+1$ points of P forming the projective group PG are even, but they form a small subgroup of the group of all $(p+1)!/2$ even permutations of the $p+1$ points of P.

Example: For $p = 5$, there are 360 even permutations of the 6 points of P, and only 60 elements in the projective group PG.

The problem is *to combinatorially describe the projective permutations* (*or the geometric structure of* P *preserved by these permutations of its* $p+1$ *elements*).

The projective transformations preserving one point of P form a subgroup of the p-affine transformations, having naturally the structure of *p-Lobachevskian plane*. In the affine coordinate, the fixed point being ∞, these affine transformations are

$$\{x \mapsto ax + b\}, \quad a = c^2, \quad c \neq 0.$$

Their number is $p(p-1)/2$. The condition that the coefficient a is a quadratic residue is the $\bmod p$ version of the choice of upper half-plane ($a > 0$) in the real Lobachevskian plane model. Inequalities should be replaced by the quadratic residue properties in p-calculus.

The combinatorial properties of these special (affine) permutations are not too difficult to understand in terms of the Lobachevsky geometry.

However, to transfer this description to the case of other choices of fixed points (better to avoid mentioning the fixed points in the description) is not easy, and I needed long explicit calculations to do it even for $p = 5$, which case leads to nice answers. In this case, the projective group permuting the 6 points of P is isomorphic to the group of even permutations of some 5 objects (which are the *Kepler cubes* of the corresponding *dodecahedron surface*).

But I do not know whether one might find such a nice description of the group of projective permutations of a finite projective line for greater values of p, except $p = 7$ where one is led to the theory of non-simply-connected regular polyhedra instead of the dodecahedron.

The ratio of the order of the group of even permutations of the $p+1$ points of P to the order of the group of projective permutations on P is equal to

$$\frac{(p+1)!}{2} : \frac{p(p^2+1)}{2} = (p-2)!,$$

which might be interpreted as the number of *cyclic orders* of $p-1$ elements.

It would therefore be nice to find a set X of $p-1$ elements associated with P whose cyclic order is preserved by the projective permutations (being disturbed by other even permutations of the $p+1$ points of P acting naturally on X).

To construct X, one might delete some two chosen points of P. The affine coordinate, for which the two chosen points are 0 and ∞, provides the natural cyclic order on X (preserved by the projective permutations fixing the chosen points).

For a different choice of two points, one obtains a new cyclic order on a new set of $p-1$ points of P. The problem is *to combinatorially describe this new cyclic order in terms of the old one*.

One can relate the dodecahedron structure associated with the group $G = \mathrm{SL}(2,\mathbb{Z}_p)$, $p=5$, to the finite projective line P by the following construction starting with any choice of a prime number p.

Let us find the elements of order p in G. An example is given by the Jordan matrix

$$J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad J^p = 1 \quad \text{in } G.$$

The solutions of the equation $A^p = 1$ in G are just the matrices with trace 2 in G. Their number is p^2 (including the p^2-1 matrices of order p and the identity matrix 1). The elements of order $p=5$ describe the rotations of the pentagonal faces of the dodecahedron constructed from G with $p=5$. One should generalize this geometry to the case $p>5$. For $p=7$, the dodecahedron must be replaced by a polyhedral surface of genus 3.

All elements of order p in G are conjugated either to J (there are $(p^2-1)/2$ such matrices) or to J^b, b being a quadratic nonresidue mod p (the same number of matrices).

An element of order p is sent to a point of the finite p-projective line P, the element being associated with the direction of its eigenvector. The preimage of a point contains $p-1$ elements of order p and is equipped with a natural cyclic order.

In the case $p=5$, the six points of P are interpreted as the six pairs of parallel faces of the dodecahedron. However, to obtain the combinatorial description of their projective permutations (for $p=5$), one has to permute the five Kepler cubes which are missing in the general case $p>5$ (except the case $p=7$ studied in my paper in *Russian Math. Surveys*, 2003 quoted above).