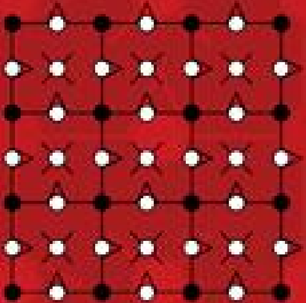
Dynamics, Statistics and Projective Geometry of Galois Fields

V. I. ARNOLD



CAMBRIDGE

CAMBRIDGE www.cambridge.org/9780521872003

This page intentionally left blank

Dynamics, Statistics and Projective Geometry of Galois Fields

V. I. Arnold reveals some unexpected connections between such apparently unrelated theories as Galois fields, dynamical systems, ergodic theory, statistics, chaos and the geometry of projective structures on finite sets. The author blends experimental results with examples and geometrical explorations to make these findings accessible to a broad range of mathematicians, from undergraduate students to experienced researchers.

V. I. Arnold was Professor of Mathematics at the Université de Paris IX (Paris-Dauphine) and at the Steklov Mathematical Institute in the Russian Academy of Sciences until his death in 2010.

Dynamics, Statistics and Projective Geometry of Galois Fields

V. I. ARNOLD

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521872003

First published 2011

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data
Arnold, V. I. (Vladimir Igorevich), 1937–2010.
The dynamics, statistics, and projective geometry of Galois fields / V. I. Arnold.
p. cm.
Includes index.
ISBN 978-0-521-87200-3 – ISBN 978-0-521-69290-8 (pbk.)
1. Finite fields (Algebra) 2. Galois theory. I. Title.
QA247.3.A76 2010
512′.32 – dc22 2010031765

ISBN 978-0-521-87200-3 Hardback
ISBN 978-0-521-69290-8 Paperback

Some words about Vladimir Igorevich Arnold

As scientist, Vladimir Igorevich Arnold was among the most influential and greatest mathematicians of the XX century. His discoveries, conjectures and challenging problems strongly influenced the development and determined the modern state of such domains in mathematics as singularity theory, dynamical systems, real algebraic geometry, symplectic and contact geometry, symplectic and contact topology, KAM theory, qualitative theory of differential equations, mechanics and many others. According to the data of 2009, he was the most cited Russian scientist, being cited in papers of mathematics, physics, astronomy, chemistry, biology and even medicine. A small planet discovered in 1981, registered under # 10031, was named Vladarnolda after him – making him the only mathematician who has had such a distinction in life! Lots of mathematicians around the world are and have been publishing scientific papers on his conjectures and problems.

The authors of these lines were his students and are representatives of Arnold's Moscow and Paris schools, cities where he was professor and had a very active seminar, with lots of students. As professor, Arnold was doing extremely careful reading and critical corrections of our texts, pointing out all words or sentences that could be misunderstood. Sometimes, he was proposing deeper statements of the results, conjecturing new "theorems" (whose statements were often true, with slight modifications,) or improving the general redaction of the text. In particular, the first article of each one of us was almost entirely written by him (as his first paper was almost entirely written by Kolmogorov): he corrected the article three or four times, the size of his corrections being each time similar to the size of the article! In his seminar he was always proposing new problems to us, often leading to new topics. To prepare his students (or any mathematician attending to his seminar) to work on his problems, sometimes he explained the interconnections of those problems with different domains of mathematics and sketched the ways in which such connections could be used. Other times he explained the essential elements of the corresponding theory, pointing out the possible difficulties and making a proper choice and detailed study of relevant examples (he claimed that examples teach more than a formal proof of a result). After Arnold's problems a great number of publications were written by his students or by other mathematicians participating in his seminar. For several of those articles the main idea was due to him, but he never signed any such paper, nor any paper of his students. Besides his brilliant and visionary mind, Arnold was extremely generous. We learnt from him much more than mathematics and to be his student was a fascinating, enriching and life-changing experience.

Arnold's qualities as scientist and professor are reflected in his numerous books, many of them forming a golden fund of mathematical educational literature. His special style of writing (very easy to recognise and difficult to reproduce) is an amazing unity of clearness and profoundness that allowed to him to explain in an accessible way the theories standing on the very foreground of modern science, and in which a committed avoidance of useless and redundant formalism is a point of principle. Following the arguments of Arnold any thoughtful reader can readily reconstruct the details corresponding to his or her mathematical background and conception. Reading of his books turns into a fascinating pastime that is almost impossible to interrupt.

Arnold's books are equally interesting and useful to both working mathematicians and physicists as well as to students and teachers. Such books as "Ordinary Differential Equations" or "Mathematical Methods of Classical Mechanics" became bestsellers of mathematical literature. Arnold passed away the 3rd of July 2010 when the present book was already prepared for publication. We hope that it will also find a delightful response of many readers and will stimulate them to read Arnold's mathematical literature.

Maxim Kazarian and Ricardo Uribe-Vargas

Contents

Preface

This book derives from a 2-hour-long presentation to Moscow high-school students at the Moscow State (Lomonosov) University MGU, in November 2004. It is a translation from the Russian of *The Dynamics, Statistics and Projective Geometry of Galois Fields*[†], which was itself based on the earlier article *Geometry and Dynamics of Galois Fields*.[‡] It describes some astonishing recent discoveries of the relations between Galois fields, dynamical systems, ergodic theory, statistics and chaos, as well as of the geometry of projective structures on finite sets.

Most of these recent discoveries encapsulated empirical studies, and some of the conjectures suggested by these numerical experiments are still unproved, despite the fact that their simple statements make them quite accessible to high-school students (who can study them empirically, thanks to computers).

Together with these continuing empirical studies, it would be nice to investigate some of the remaining theoretical questions, such as the natural problem of the intrinsic characterisation of projective permutations among all the permutations of a finite set. We ought to be able to understand those geometrical features of some special permutations of a dozen points that make these special permutations projective, thereby distinguishing them from non-projective permutations.

The author thanks the audience for many helpful remarks and hopes to extend the collaboration with the readers of the present book. The author looks forward to there being many contributions to this young domain of mathematics

[†] Moscow Center for Continuous Mathematical Education, Moscow, 72pp.

[‡] *Russian Mathematical Surveys*, **59** (6), (2004) (pages 23–40 in the Russian version).

(including, one hopes, the discovery of applications of Galois fields beyond mathematics).

The author thanks G. Capitanio for help in typing the LaTeX file of this text and the figures. These studies were supported in part by RFBR grant 05–01–00104.

1
What is a Galois field?

A *Galois field* is a field that has a finite number of elements. Such fields belong to the small quantity of the most fundamental mathematical objects that serve to describe all other mathematical structures and models.

Another example of such fundamental objects is the well-known prime numbers:

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, \dots, 997, 1009, \dots ;$$

these are the positive integers that each have only two integer divisors (namely 1 and the number itself). By convention we do not take the number 1 to be prime.

An immediate natural question, to which this notion leads, is already rather difficult: *is the set of all the primes finite*? In other words, can the above sequence of primes be continued indefinitely?

The answer to this question was discovered in antiquity: *the sequence of prime numbers is infinite*, i.e. there is no maximal prime number.

To prove it, assume the opposite, i.e. that there is a maximal prime p, and consider the number

$$(2 \times 3 \times 5 \times \cdots \times p) + 1 \, .$$

This has remainder (residue) 1 when we divide it by any prime number $2, 3, \dots, p$. This number (which is greater than p and so, by assumption, is not prime) is not, therefore, divisible by any of them. Hence, it has a prime divisor which is greater than p – a contradiction. Therefore, *there is no maximal prime number p*.

This remarkable mathematical result avoids the question that interests us, as scientists, most: *how often* are primes encountered in the sequence of all the natural numbers $\{1, 2, 3, 4, 5, 6, \dots\}$? Do the intervals between consecutive prime numbers grow as the numbers we consider become large? What is the millionth prime expressed as a decimal number?

The first scientist to study this problem was Adrien Marie Legendre (1752–1833), who had considered (in the eighteenth century) tables of primes up to 10^6 and who had discovered empirically the following *law of the decline in density of the primes*: the average distance between consecutive prime numbers of order of n, grows with n like $\ln n$ (here, ln is the natural logarithm, which is the logarithm to the base $e \approx 2.71828\ldots$, where the 'Euler number' e is

$$e = \lim_{k \to \infty} \left(1 + \frac{1}{k}\right)^k = \sum_{m=0}^{\infty} \frac{1}{m!} \, .$$

Thus, for example, $\ln 10 \approx 2.3$, and the average distance between consecutive primes close to 10 is slightly greater than 2, since

$$7 - 5 = 2 \, , \; 11 - 7 = 4 \, , \; 13 - 11 = 2 \, .$$

The primes in the region of $n = 100$ are 89, 97, 101, 103, so their average separation is $4\frac{2}{3}$. This distance should be compared with $\ln 100 = 2 \ln 10 \simeq 4.6$ from Legendre's law, and it is thus confirmed satisfactorily even for $n = 100$.

Of course, the existence of pairs of *twins* (that is, of prime pairs whose difference is 2, such as 5 and 7, 17 and 19, 29 and 31) contradicts the expected increasing separation of consecutive prime numbers, provided that the number of such twins is infinite, which is conjecturally true. (This conjecture is one of the most celebrated unproved statements of modern number theory.)

Unfortunately, Legendre's empirical observations were not appreciated by the mathematical community of the time, since 'he had proved nothing, but only considered some millions of examples'. It is true that he succeeded in 'deducing' his law from empirical statistical observations, but he was unable to provide a strict mathematical proof that in the asymptotic limit, as $n \to \infty$, the average distance between primes coincides with his proposed value of $\ln n$.

Kolmogorov said to me several times, concerning his studies on hydrodynamical turbulence: 'do not try to find in my works any theorem that proves the statements I make: I am unable to deduce them from the basic (Navier–Stokes) equations of hydrodynamics. My results on the solutions of these equations are not *proved*, but they are *true*, which is more important than all proofs.'

The first person who appreciated Legendre's discoveries was the Russian mathematician Tchebyshev. He first proved that even if the average distance between consecutive primes in the neighbourhood of a large number n does not behave asymptotically as $\ln n$, its relation to this Legendre value remains *bounded*, i.e. the average distance lies between $c_1 \ln n$ and $c_2 \ln n$ (where $c_1 < c_2$ were explicitly calculated).

Later, he proved more: provided that any oscillations between the above limits would die out as n grows, implying that the average distance to the asymptotic value would be $c \ln n$ for some constant c, then *the constant c cannot be different from* 1.

This is not yet sufficient to *prove* the Legendre asymptotic formula, since there remains the possibility of non-vanishing oscillations between $c_1 \ln n$ and $c_2 \ln n$, therefore, never leading to the $c \ln n$ behaviour.

However, about 100 years after Legendre's discovery, two celebrated mathematicians, Hadamard (from France) and de la Vallée Poussin (from Belgium), proved that the oscillations do indeed die out for $n \to \infty$, yielding the $c \ln n$ asymptotic behaviour of the average distance between the consecutive primes in the neighbourhood of n.

The mathematical community claims, therefore, that Hadamard and de la Vallée Poussin made a great discovery concerning the distribution of large prime numbers.

It seems to me that this claim is rather unfair. These great mathematicians simply proved the *existence* of the distribution law.

Both 'scientific' facts, namely the asymptotic proportionality, to $\ln n$, of the average separation, and that the constant of proportionality equals 1, were discovered by Legendre and Tchebyshev, to whom one should attribute the great discovery of the law of distribution of primes described above.

In this book, therefore, I shall follow Legendre rather than Hadamard: I shall discuss empirical numerical observations that suggest some new (and astonishing) natural laws whose transformation to mathematical theorems might have to wait some hundred years (as happened in the case of the law of distribution of primes), despite the fact that the discovery of these new laws is quite within the reach of high-school students, even without the use of computers, although using computers might accelerate numerical experiments[†].

In addition to the prime numbers, another example of a fundamental mathematical object is provided by *regular polyhedra* (also called 'Platonic solids', even though Plato did not discover them). There are five such bodies: the tetrahedron (with 4 faces), the octahedron (with 8 faces), the cube (with 6 faces), the icosahedron (from the Greek 'icos' for its 20 faces) and the dodecahedron (from the Greek 'dodeca' for its 12 faces) – see Figure 1.1.

[†] I used no computers in the experiments that led me personally to the results below: my students, who verified that machines gave the same answers as I did, discovered that my calculations contained many fewer mistakes than those done by using computers.

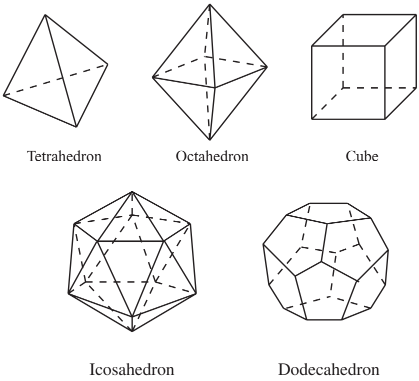


Figure 1.1 Regular polyhedra

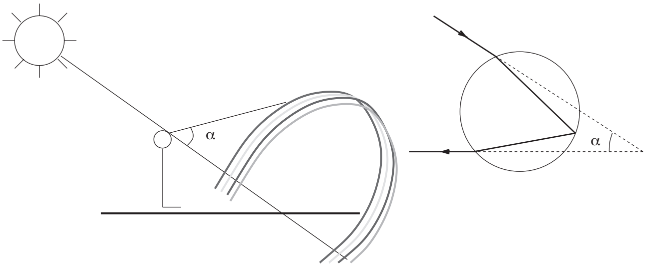


Figure 1.2 The origin of rainbows

The dodecahedron was used by Kepler to describe the orbital radius law of planets in the solar system.

The regular polyhedra are related in a strange way to a domain of physics which seems to be quite different – namely the theory of *optical caustics*, which provides, for instance, an explanation of the phenomenon that the angular radius of a rainbow is $\alpha = 42^\circ$, and describes how galaxies are concentrated at large scales in the universe.

Kolmogorov explained that the special beauty of mathematical theories is due to the way they reveal *unexpected relations between quite different natural phenomena* (say, between the theories of the electric and magnetic fields as described by Maxwell's equations).

In distinction to the fundamental objects in the examples above, the applications of Galois fields to the natural sciences are yet to be discovered. I hope that they will appear rather soon, and I would like to shorten the time till then by giving a geometric presentation of Galois field theory. My description is

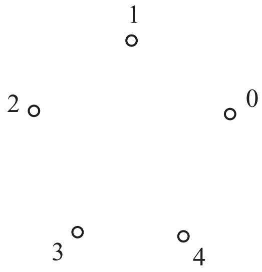


Figure 1.3 A finite circle: the Galois field $\mathbb{Z}_5$

closer to the scientific approach than to the axiomatic–algebraic superabstract style that dominates current presentations of this algebraic theory.

The simplest example of a Galois field is the field of residues modulo a prime number p (Figure 1.3).

Thus, for $p = 2$ we get the field consisting of two elements:

$$\mathbb{Z}_2 = \{0, 1\} ,$$

with its usual arithmetic

$$0+0=0 , \quad 0+1=1+0=1 , \quad 1+1=0 ,$$
$$0\cdot 0=0\cdot 1=1\cdot 0=0 , \quad 1\cdot 1=1 .$$

This ‘binary’ arithmetic is the basis for calculating with computers, which use the binary system. Thus, the simplest Galois field is extremely useful:

$$(\text{the field } \mathbb{Z}_2) \Longrightarrow (\text{computers}) .$$

The general notion of a field is very similar to this simple example: there are two operations (called ‘addition’ and ‘multiplication’), having the usual properties of commutativity and associativity and satisfying the ordinary distributive law; and one can divide the elements of the field by any element of the field different from 0.

The residues after division by 3 form the field $\mathbb{Z}_3$, consisting of three elements $\{0, 1, 2\}$ (where $1/2 = 2$, since $2 \cdot 2 = 1$ for the residues modulo 3: $(3a + 2)(3b + 2) = 9ab + 6a + 6b + 4 = 3c + 1$).

On the other hand, the four residues after division of the integers by 4 do not form a field, since the element 2 cannot be inverted (the residue $2x$ is sometimes 0, sometimes 2, but it is different from 1, whatever the remainder x).

However, there does exist a field of four elements, though the operations are different from the above example. To find these operations is a useful exercise, one that is neither too difficult, nor too easy for a beginner.

The finite fields are called *Galois fields*, since Galois discovered the following two remarkable properties of them:

1. *The number of elements of a finite field is an integer of the form p^n, where p is a prime; and for any prime p and any natural number n there exists a finite field having just p^n elements.*

   Thus, there exist fields with

$$2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27$$

elements, but there is no field with

$$6, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26$$

elements.

2. *The field of p^n elements is defined unambiguously by the number of its elements (up to isomorphism).*

Thus, a computer using the field $\mathbb{Z}_2$ at Moscow, and another computer, working in Paris, might each use a different copy of this field. The Parisian might denote the elements of the field by α and β (instead of 0 and 1), and define the operations according to the table:

$$\alpha + \alpha = \beta + \beta = \beta\ , \quad \alpha + \beta = \beta + \alpha = \alpha\ ,$$
$$\alpha \cdot \alpha = \alpha\ , \quad \alpha \cdot \beta = \beta \cdot \alpha = \beta \cdot \beta = \beta\ .$$

But this field is isomorphic to the Moscow field of residues $\mathbb{Z}_2$, differing only in the notation $\alpha \sim 1$ and $\beta \sim 0$. The fact that phenomena are independent of notation is a deep notion, one that is also at the foundation of relativity theory and so the whole of relativistic physics.

I shall not give here proofs of the above-formulated existence and uniqueness theorems for the field of p^n elements. *I shall instead describe, by explicit tabulation, the operations in this field.* Strangely, I have not seen in published form the science-oriented description of finite fields that I present below.

Every field contains the 0 element (zero), which has the property of not changing any element to which it is added. All the other elements of the field form *the multiplicative group of the field* (i.e. a group under multiplication) since each non-zero element can be inverted.

This group is always cyclic: there exists an element A of the field such that every non-zero element of the field has the form A^k, where $1 \leq k \leq p^n - 1$ for the field of p^n elements.

I shall not prove the cyclic property (though its proof is not too difficult), since this result adds to the theory only the following statement, loved

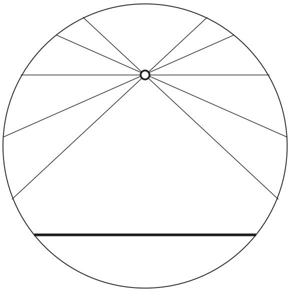


Figure 1.4 Lobachevsky plane

by axiomatisers: *the only finite fields are those with a cyclic multiplicative subgroup*.

In other words, we can consider the theory, explained below, as describing finite fields with an additional axiom: namely, the multiplicative group of the field is cyclic, or in other words a *primitive element* exists whose powers provide all the non-zero elements of the field.

The *absence of any different finite field* is a nice addition to this theory, but the theory itself does not depend on this additional property of our axioms.

It is worthwhile to observe that the exaggerated attention to the difficult study of the independence of axioms makes the algebraic and abstract theories of mathematicians unnecessarily hard and intimidating for scientists.

Thus, the *Lobachevsky plane* is simply the interior disc of the unit circle, whose interior points are called ‘Lobachevsky points’, and whose ‘Lobachevsky lines’ are chords of the unit circle. The boundary circle (which does not belong to the Lobachevsky plane) is called ‘absolute’.

It is very easy to see that these objects (forming the so-called *Klein model* of the Lobachevsky plane – although, of course, they had been invented by A. Cayley) – satisfy all but one of the axioms of Euclidean geometry (‘there exists one, and only one, line connecting two given points’, etc.). The exception is the ‘parallel axiom’: *there exist an infinity of Lobachevsky lines going through a given Lobachevsky point and having no common Lobachevsky points with a given Lobachevsky line that does not contain the given Lobachevsky point* (that is, an infinity of chords, see Figure 1.4).

This list of obvious scientific facts can be completed by a (difficult) formal theorem: *there exists no Lobachevsky plane other than the Klein model described above*. Of course, this is true up to isomorphisms: the theorem states that the axioms for the Lobachevsky plane imply that this plane is isomorphic to the Klein model.

It is interesting that Lobachevsky was unable to prove his main and quite remarkable statement: *the parallelism axiom of Euclidean geometry is independent of the other axioms*; that is, it cannot be deduced from them.

The model described above (and invented many years after Lobachevsky worked) proved just this independence result.

Indeed, *if one could use the failure of the Euclidean parallels axiom to deduce a contradiction* (which contradiction would indeed prove the axiom), *then the model would also be false providing therefore a contradiction within the usual Euclidean geometry* (concerning the ordinary geometry of the chords of a circle).

The proofs of fundamental mathematical facts are, in many cases, much simpler than the formal details that make mathematics textbooks so difficult.

2

The organisation and tabulation of Galois fields

Multiplication in a Galois field that consists of n elements, 0 and $\{A^k\}$, $1 \leq k \leq n-1$, is simply the addition of the 'logarithms' k of the elements (where we consider these logarithms as the residues of the numbers k modulo $n-1$):

$$0 \cdot A^k = 0\,, \quad A^k \cdot A^\ell = A^{k+\ell};$$

if $k + \ell > n - 1$, one replaces the sum by $k + \ell - (n-1)$ to reduce the sum to a value smaller than n.

It remains to define the addition operation. Denoting the element A^k of the field by the sign k, we arrive at the following *tropical operation* $*$ over these logarithms:

$$A^k + A^\ell = A^{k*\ell}\,.$$

The modern term 'tropical', taken by me to mean 'exotic', is used when one lowers the level of the algebraic operations, transforming multiplication to addition, and replacing addition by the lower-level 'tropical addition' operation, with respect to which the normal addition is distributive, as is normal multiplication with respect to normal addition:

$$x(y+z) = xy + xz \quad \text{is replaced by} \quad x + (y * z) = (x+y) * (x+z)\,.$$

An example of such tropical addition is the operation $x * y = \max(x, y)$ for the real numbers. One can obtain this tropical operation from normal addition by using logarithms accompanied by the short wave asymptotic expansion of quantum mechanics, when the wave length h approaches 0. The relation

$$\frac{x *_h y}{h} = \ln(e^{x/h} + e^{y/h})$$

defines the tropical addition operation $*_h$, tending to $\max(x, y)$ as $h \to 0$.

While all these things are obvious, they imply a non-obvious ‘tropical’ conclusion: replacing multiplication and addition operations with their tropical versions (i.e. addition and maximum), one can transform many formulas and theorems of calculus (such as Fourier series theory) into their (non-evident) ‘tropical’ versions, providing interesting results in convex analysis and linear programming.

Consider for simplicity the case of the field F of $z = p^2$ elements. It contains the ‘scalar’ elements $1, 2 = 1 + 1, \ldots$. Since this field is finite, one of the sums must coincide with the other. Hence, for some m, the sum of m 1s (equal to the difference of the coincident sums) equals 0 i.e. $m = 1 + \cdots + 1 = 0$. We shall suppose the number m to be the minimal value for which this statement is true.

We shall now prove that $m = p$. We will say that each element x is equivalent to any element of the form $x + 1 + \cdots + 1$, where the number of 1s is at most m. Each equivalence class consists of m elements, and these classes are disjoint. Therefore the number m of scalar elements is a divisor of the number p^2 of elements of the field. Thus, m is either p or p^2.

The second case is impossible. Consider the scalar element $x = 1 + \cdots + 1$ (p times). This element of the field of p^2 elements has no inverse element, since no integer of the form pq leaves the residue 1 when divided by p^2. Therefore, $x = 0$ and the number of scalars is thus $m = p$.

Consider the element 1 together with a primitive element A of our field. Adding each of them fewer than p times, we create the p^2 sums $uA + v1$. All these elements are different (otherwise we would obtain $A = (-v/u) \cdot 1$, and therefore all the elements of the field would be scalars, which is impossible, since the number of scalars is p, which is smaller than p^2).

Thus, the field of p^2 elements consists exactly of linear combinations $F = \{uA + v1\}$ with coefficients $u \in \mathbb{Z}_p$, $v \in \mathbb{Z}_p$.

In this sense we have distributed all the elements of the field in the form of a $p \times p$ square (or rather of the ‘finite torus’ $\mathbb{Z}_p^2$ of Figure 2.1, this being the 2-plane over the field $\mathbb{Z}_p$).

So we have filled the $z = p^2$ cells of this finite torus with the p^2 ‘logarithmic symbols’ $\{\infty; 1, \ldots, z-1\}$, where the symbol k, which is a residue modulo $z - 1$, denotes the element A^k of the field F, the symbol ∞ representing[†] the zero element of the field.

This filling process provides a simple interpretation of the tropical operation $*$; namely, the sum of the elements of the field that correspond to the symbols

[†] During my lecture, the students suggested denoting $\ln 0$ by $-\infty$, but I kept the symbol ∞ since I do not know whether $A > 1$ in F.

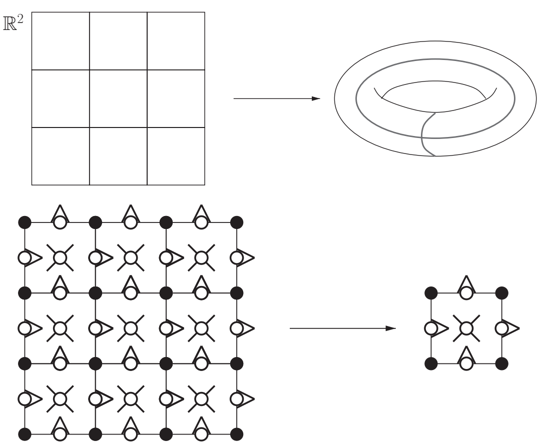


Figure 2.1 The continuous torus and the finite torus consisting of four points

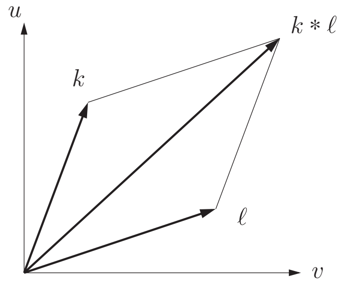


Figure 2.2 Tropical addition of the numbers k and ℓ in the field table

k and ℓ, given by

$$A^k = u'A + v'1\,, \qquad A^\ell = u''A + v''1\,,$$

is $(u' + u'')A + (v' + v'')1 = A^{k*\ell}$.

Therefore (see Figure 2.2), *the symbol $k * \ell$ fills the cells of the field table with the vector sum of the places of the symbols k and ℓ: the addition operation of the field F (which consists of p^2 elements) is represented by the vector addition of the places of the summed elements in the field table.*

Thus, all we need to describe the field of $z = p^2$ elements is to calculate the places (u_k, v_k) of the elements

$$A^k = u_k A + v_k 1 \qquad (1 \le k \le z - 1)$$

in the field table.

This calculation is an easy extension of the method of recursive construction of the Fibonacci numbers a_k, i.e. the sequence $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$, $a_{k+2} = a_{k+1} + a_k$, which describes the population growth of rabbits.

Thus, suppose that in the field F we have

$$A^2 = \alpha A + \beta 1 \ , \qquad (\alpha \in \mathbb{Z}_p \ , \ \beta \in \mathbb{Z}_p) \ . \tag{2.1}$$

Then, we find in F the relation

$$A^3 = A(\alpha A + \beta 1) = \alpha(\alpha A + \beta 1) + \beta A = (\alpha^2 + \beta)A + \alpha\beta 1 \ .$$

Continuing in this way, we get the recursive relation giving the places of the elements A^k in the field table:

$$u_{k+1} = \alpha u_k + v_k \ , \quad v_{k+1} = \beta u_k \ . \tag{2.2}$$

Therefore, the two residues α and β (modulo p) provide, in turn, the places (u_k, v_k) of all the elements A^k in the field table.

To obtain the table, we only have to choose the values of the parameters α and β. One should choose them in such a way that first, $A^{p^2-1} = 1$ (that is, $u_{p^2-1} = 0$, $v_{p^2-1} = 1$); and second, all the preceding vectors (u_k, v_k) $(1 \leq k < p^2 - 1)$ are different from the vector $(0, 1)$.

In principle, one could try, in turn, all the p^2 pairs of residues (α, β) to find convenient values of the parameters. The number of trials is not even that large. For instance, if $p = 5$ both conditions above are fulfilled by the pair $\alpha = \beta = 2$.

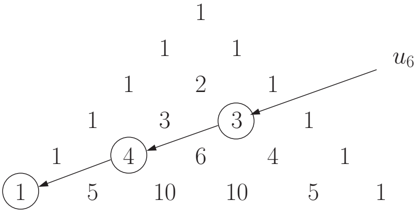
However, one can considerably accelerate the process using *Pascal's triangle* of binomial coefficients. For it is easy to prove the following explicit formula[†] for the recurrent relations (2.2):

$$u_k = \sum \alpha^s \beta^t C^t_{s+t} \ , \tag{2.3}$$

where the powers s and t are related by the homogeneity condition for the coefficient u_k in A that is implied by the condition (2.1). This condition provides the weights ($\deg \alpha = 1, \deg \beta = 2$), implying, for $\deg u_k = k - 1$, the homogeneity relation $s + 2t = k - 1$ for the degrees s and t of the monomials in the formula (2.3) for the quantity u_k.

For instance, for $k = 6$, Pascal's triangle provides the following values for the coefficients in (2.3):

[†] The notation C^t_{s+t} simply means the 'number of combinations'.



Therefore, the quantity u_6 is represented as the sum of three monomials of weight 5:

$$u_6 = 3\alpha\beta^2 + 4\alpha^3\beta + 1\alpha^5 \ .$$

Using this algorithm, it took me only half an hour to calculate the places of the 24 non-zero elements A^k of the field consisting of 25 elements. The resulting field table is

$p = 5$

u						
4	**13**	15	**5**	16	20	
3	**7**	10	9	14	**23**	
2	**19**	**11**	2	21	22	
1	**1**	8	4	**17**	3	
0	∞	24	18	6	12	
	0	1	2	3	4	v

Example $A^{10} = 3 \cdot A + 1 \cdot 1$, $A^{19} + A^8 = A^{10}$.

Remark The centre of symmetry of the table, denoted by the sign '$\circ$', has the following easy-to-prove property: $k - \ell = 12 \pmod{24}$ whenever the places of the symbols k and ℓ are situated symmetrically with respect to this centre (on the finite torus).

For instance, $21 - 9 = 12, 17 - 5 = 12, 24 - 12 = 12$: this value would be equal to $(z - 1)/2$ for a field of z elements.

The reason for this symmetry is the evident identity $A^{12} = -1$: that is, $u_{12} = 0$, $v_{12} = 4$.

And this symmetry allows us to reduce the process of constructing the field table by a factor of two, making it twice as fast: it suffices to find the coordinates (u_k, v_k) of the symbols $k \leq z/2$ in the case of a field having $z = p^n$ elements.

The field table may be interpreted as follows. Multiplication of the elements of the field by A acts as a linear operator on A^k on the plane of the table:

$$A^k \cdot 1 = u_k A + v_k 1 \ ,$$
$$A^k \cdot A = u_{k+1} A + v_{k+1} 1 \ .$$

Therefore, the matrix of this linear operator on the plane with coordinates u and v and equipped with the basis $(1, A)$, has the form

$$(A^k) = \begin{pmatrix} v_k & v_{k+1} \\ u_k & u_{k+1} \end{pmatrix} \ .$$

For $k = 1$, this matrix is equal to

$$(A) = \begin{pmatrix} 0 & \beta \\ 1 & \alpha \end{pmatrix} ; \qquad \left(\text{equal to } \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} \text{ for } p = 5 \right) \ .$$

The relation (2.1) is simply the characteristic equation for the matrix (A).

Since the operator of the multiplication by A^k is the kth power of multiplication by A, the matrix (A^k) is the kth power of the matrix (A).

Therefore, the *construction of the field table provides a representation of the field consisting of p^2 elements by the second-order matrices* (A^k)*, whose elements belong to* $\mathbb{Z}_p$.

The field operations are represented by matrix addition and multiplication:

$$(A)^k \cdot (A)^\ell = (A)^{k+\ell} \ ,$$
$$(A)^k + (A)^\ell = (A)^{k*\ell} \ .$$

For the field consisting of $z = p^n$ elements, a similar construction provides a representation by nth-order matrices with elements in the field $\mathbb{Z}_p$. Some examples where $n = 3$ are listed later in Chapter 8.

For the fields of p^2 elements, where $p = 7$, 11 and 13, the calculations, quite similar to those described above for $p = 5$, yield the following results:

$$\begin{array}{cc} p = 7 & p = 11 \\ (A) = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} & (A) = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} \end{array}$$

$$p = 13$$
$$(A) = \begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix} \ .$$

The resulting *table for the field of $p^2 = 49$ elements* fills the finite torus $\mathbb{Z}_7^2$ with the following residues (modulo 48):

$p = 7$

u								
6	**25**	44	**7**	30	3	45	42	
5	9	**35**	28	**29**	39	26	14	
4	**17**	**37**	22	36	34	**43**	**47**	
3	**41**	**23**	**19**	10	12	46	**13**	
2	33	38	2	15	**5**	4	**11**	
1	**1**	18	21	27	6	**31**	20	
0	∞	48	32	40	16	8	24	
	0	1	2	3	4	5	6	v

The table of the field of $p^2 = 121$ *elements* fills the finite torus $\mathbb{Z}_{11}^2$ with the residues (modulo 120):

$p = 11$

u												
10	**61**	**11**	15	76	22	**43**	78	**53**	62	56	105	
9	25	42	95	**17**	99	26	40	20	106	69	**7**	
8	**13**	94	14	**83**	115	8	87	30	57	28	5	
7	**109**	4	6	104	**59**	70	**101**	33	63	**91**	110	
6	**37**	32	**29**	**19**	52	**107**	81	38	54	118	111	
5	**97**	51	58	114	98	21	**47**	112	**79**	**89**	92	
4	**49**	50	**31**	3	93	**41**	10	**119**	44	66	64	
3	**73**	65	88	117	90	27	68	55	**23**	74	34	
2	85	**67**	9	46	80	100	86	39	**77**	35	102	
1	**1**	45	116	2	**113**	18	**103**	82	16	75	**71**	
0	∞	120	84	72	48	96	36	108	12	24	60	
	0	1	2	3	4	5	6	7	8	9	10	v

Bold numbers in these tables represent the generators A^k of the multiplicative group of the field: they correspond to the values of k that are relatively prime to $z - 1 = p^2 - 1$ which equals 120 in the present case, $p = 11$.

The table of the field of $p^2 = 169$ *elements* fills the finite torus $\mathbb{Z}_{13}^2$ with the residues (modulo $168 = 2^3 \cdot 3 \cdot 7$) in the following table:

$p = 13$

u														
12	**85**	45	161	165	**13**	76	58	**47**	158	122	**23**	166	64	
11	15	**145**	**143**	88	91	52	**95**	**121**	111	96	6	162	156	
10	141	10	132	**101**	**79**	114	49	54	**103**	**53**	120	46	69	
9	**113**	51	75	**41**	**73**	26	18	104	21	92	150	86	**25**	
8	**127**	32	39	40	100	87	164	**55**	106	**89**	35	**65**	118	
7	**71**	152	108	33	62	**151**	**31**	50	9	144	44	**167**	147	
6	**155**	63	**83**	128	60	93	134	**115**	**67**	146	117	24	68	
5	**43**	34	**149**	119	**5**	22	**139**	80	3	16	124	123	116	
4	**29**	**109**	2	66	8	105	20	102	110	**157**	**125**	159	135	
3	57	153	130	36	**137**	**19**	138	133	30	**163**	**17**	48	94	
2	99	72	78	90	12	27	**37**	**11**	136	7	4	**59**	**61**	
1	**1**	148	82	**107**	38	74	**131**	142	160	**97**	81	77	129	
0	∞	168	98	56	28	42	154	70	126	112	140	14	84	
	0	1	2	3	4	5	6	7	8	9	10	11	12	v

Remark While the field is defined unambiguously by the number of its elements, the *table* of this field is not defined by this number, since it depends upon the choice of the multiplicative generator A of the group of the non-zero elements of the field. Instead of the generator A, one might choose a different primitive element, $\tilde{A} = A^k$ (which is primitive exactly when k is relatively prime to the number $z - 1$ for a field of z elements).

Given a natural number m, the subset formed by the elements of the ring of residues modulo m that are relatively prime to m is a multiplicative group of the ring $\mathbb{Z}_m$, which we call the *Euler group* $\Gamma(m)$. Equivalently, we can define the *Euler group* $\Gamma(m)$ as the set formed by the elements of $\mathbb{Z}_m$ that have a multiplicative inverse.

If we choose a primitive element A in a field of order z, we can identify the set of all primitive elements with the elements of the Euler group $\Gamma(z - 1)$, by making A^k correspond to k in $\Gamma(z - 1)$.

We will discuss the influence of the choice of the primitive element A on the above constructions in Chapter 7: these investigations lead to some astonishing facts about the projective geometry of finite sets (see Chapters 6 and 7).

3

Chaos and randomness in Galois field tables

Looking at the tables of Galois fields in the previous chapter, one has the impression that the ways of filling them by the integers from 1 to $z - 1$ (where z is the number of elements in the field, taken to be equal to p^2 in our examples) behave in some *random* kind of way: it is difficult to guess the place of the next symbol $k + 1$ given the place of the preceding symbol k.

Attempts to formulate this empirical observation as a mathematical statement lead to hundreds of conjectures. Perhaps most of these conjectures will become interesting theorems in the future: at present, only a few of them have been proved.

I will now describe the general scheme for formulating the ‘randomness’ conjectures.

To begin with, note that genuinely random fillings have several properties known from the theory of probability and stochastic processes.

To check the ‘randomness’ of the field table filling, choose one of these properties and check whether the ‘quasi-random numbers’ that fill the table do approximately satisfy it.

Arguing in this way, we arrive at a conjecture that claims that the chosen randomness property is approximately fulfilled by the matrix of the field of $z = p^n$ elements, and that the approximation gets better and better as we increase the prime number p for fixed n, i.e. the number z of elements. In the limit $p \to \infty$, the property is conjectured to be fulfilled exactly.

Thus, to fix the mathematical formulation of the quasi-randomness conjecture one has to describe exactly the chosen property. Since many such properties exist, one gets many conjectures. I shall present below a short list of the simplest examples, which are already non-trivial and interesting, despite their simplicity: any high-school student can check these conjectures empirically, for fixed p, even by hand.

Let us start with an example. Suppose that the whole table is subdivided into two disjoint parts and write G for one of these parts. We count the numbers k that fill the table and occur in G.

For a random filling the number N of occurrences of G among m trials is proportional to the volume (i.e. to the area in the two-dimensional case) of the domain G:

$$\frac{N}{m} \approx \frac{|G|}{z} ;$$

here, z is the total volume of the table, so $z = p^2$ in the case of the field of p^2 elements.

Of course, for $m = z$ the above approximate equality is exactly fulfilled by the sequence of the elements A^k, $1 \leq k \leq m$, of the field since each cell of the table that belongs to the domain G is visited by the sequence $\{A^k\}$ just once.

Therefore, to formulate a non-trivial conjecture about the equidistribution of the elements $\{A^k\}$ in the field, one needs only to take a part of the whole sequence. Choose for this part a number ϑ strictly between 0 and 1 and consider the start of the sequence $\{A^k\}$ that consists of its firsts $m \approx \vartheta z$ members $(1 \leq k \leq m)$. Then we get the following conjecture.

The geometric progression equidistribution conjecture for the Galois field of $z = p^n$ elements

We state this as

$$\lim_{p \to \infty} \frac{N}{m} = \frac{|G|}{z} , \tag{3.1}$$

where N is the number of those first m members of the sequence $\{A^k\}$ from the field of z elements that do belong to the domain G.

I have fixed here the dimension n of the table, but one can also consider the limit $z \to \infty$, where n is not fixed.

Example *For the field of $z = p^2 = 25$ elements, choose as G the union of the first two columns of the table: $|G| = 10$, $v = 0$ or 1 in G.*

Let us take the first half of the geometric progression $\{A^k\}$, $1 \leq k \leq (12 = m)$.

Then the number of visits (counted by the field table on page 13) is $N = 5$. The deviation from the theoretical randomness criterion (3.1) is, in this case,

$$\frac{N}{m} - \frac{|G|}{z} = \frac{5}{12} - \frac{10}{25} = \frac{1}{60} .$$

Therefore, even though the prime number $p = 5$ is not that large, the approximation to equidistribution is rather good.

I have not yet been able to prove the limit theorem (3.1) in its general form, but in Chapter 4 I discuss some of the versions that have been proved.

Examples of other randomness criteria one may suggest are as follows.

Subdivide the field into two disjoint domains

$$F = G \cup H \ ,$$

whose respective numbers of elements are given by

$$|F| = z \ , \quad |G| = rz \ , \quad |H| = sz \ ,$$

where $r + s = 1$.

For a genuinely random sequence of chosen elements A_k in F the*frequencies of the jumps* from G to G, from G to H, from H to G, and from H to H for the transition to the next element of the sequence are, respectively, r^2, rs, sr and s^2.

For the geometric progression $\{A^k\}$ (which one can leave unshortened in this case: $1 \le k < z$) one would expect the frequencies of the four events $(A^k \in G, A^{k+\ell} \in G)$, $(A^k \in G, A^{k+\ell} \in H)$, and so on, to be similar.

The mixing conjecture of the geometric progression $\{A^k\}$ for the field of $z = p^n$ elements

The numbers $N(G, G)$, $N(G, H)$, $N(H, G)$ and $N(H, H)$ of occurrences of those symbols k for which $(A^k \in G, A^{k+\ell} \in G)$, $(A^k \in G, A^{k+\ell} \in H)$, and so on, are asymptotically proportional to the frequencies (r^2, rs, sr, s^2) of the random jumps:

$$\lim_{\substack{p \to \infty \\ \ell \to \infty}} \frac{N(G, G)}{z} = r^2 \ , \qquad \lim_{\substack{p \to \infty \\ \ell \to \infty}} \frac{N(G, H)}{z} = rs \ , \qquad \ldots \quad .$$

One more randomness criterion is provided by the *table variation* that measures *the differences of the symbols k between neighbouring cells of the table*. For instance, one might count the sum of the differences $|k - \ell|$. Better still, define Σ to be the sum of the cyclic distances $d(k, \ell)$ between neighbouring symbols in the table, comparing it with the similar sum for a purely random filling of the table by the symbols k, where $1 \le k < z$. Notice that $d(k, \ell)$ here means the difference between k and ℓ as residues modulo p^2 (although it could be more natural to view them as residues modulo $p^2 - 1$).

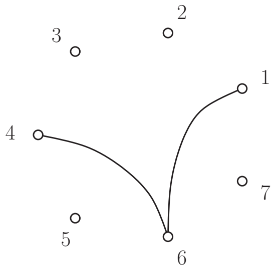


Figure 3.1 Distances of value 2 between points of a finite torus

We expect that the difference, asymptotically, of each of these two (differing) sums for the field from the mathematical expectation for a random filling would become (relatively) small for large primes p (i.e. as the number $z = p^n$ of elements of the fields grows).

For the table of the field of $p^2 = 25$ elements (see page 13), the observed averaged distance $d(k, \ell)$ between the residues k, ℓ occupying neighbouring places in the toric table is 6.41. For a truly random filling, the expectation of this distance (between the residues modulo $p^2 - 1$) would be $(p^2 - 1)/4 = 6$.

For the table of the field with $p^2 = 169$ elements (on page 16) the observed averaged distance $d(k, \ell)$ between the residues k, ℓ that are horizontal neighbours in the table equals 42.0299; whereas for random filling the expectation would be $(p^2 - 1)/4 = 42$. We take neighbouring here to mean in the sense of toric geometry: thus, for $p = 5$ the value $u = 4$ is a neighbour of $u = 0 (\equiv 5)$.

In a similar way, one can consider a different kind of variation, one that measures the distance ρ between the places of the symbols k and $k + 1$ in the table. The distance between the places can be measured using the sum of the difference of the coordinates (using the toric geometry: that is, considering the coordinates as being residues modulo p). One could consider the quantity $\varrho = \sum_k \varrho(k, k + 1)$, summing either over the cyclically closed sequence, or over the usual sequence, $1 \leq k < z$.

The averaged distance $\varrho(k, k + 1)$ between the places of consecutive residues in the toric $p \times p$ table of the field of $p^2 = 25$ elements is observed to be $2\frac{13}{24}$, whereas random filling would yield the expected average of $p/2 = 2\frac{1}{2}$.

When counting these summands one must not forget the toric geometry of the table filling $\mathbb{Z}_p^n$ with the symbols k. For instance, for $p = 7$ and $n = 1$ consider the filling of the seven consecutive places of the table by the cyclical sequence of values $k = (1, 5, 4, 2, 3, 7, 6)$ (see Figure 3.1).

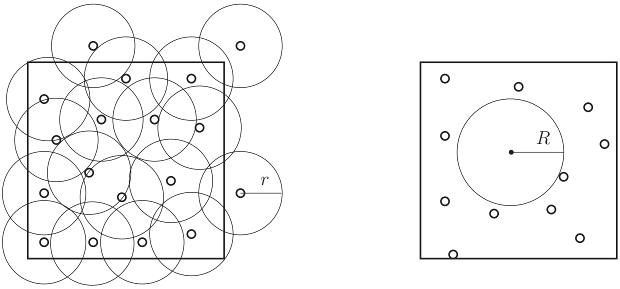


Figure 3.2 Covering balls and empty balls of a set of points

For this filling one gets (for Σ defined on the previous page)

$$\varrho = 3 + 1 + 2 + 1 + 2 + 1 + 2 = 12\,,$$
$$\Sigma = 3 + 1 + 2 + 1 + 3 + 1 + 2 = 13\,,$$

since $d(3, 7) = 3$ and $d(6, 1) = 2$ in the toric geometry of $\mathbb{Z}_7$.

The variation ϱ takes the value 12 on this cyclical sequence of the seven residues modulo 7.

For these variations, the field table randomness conjecture suggests a relatively small difference between the quantity ϱ, calculated from the table of the field of $z = p^n$ elements, and the mathematical expectation of a similar sum for a genuinely random filling of the table, provided that p (or z) is sufficiently large.

One can use here either the sum of the m distances between the m elements of a cyclic sequence, or the sum of the $m - 1$ distances between the elements of an ordinary sequence of m elements.

As further randomness characterisation of the set $\{A^k\}$ in the table one can use a quantity such as the minimal radius $r(m)$ of the balls centred at the first m points of the set that cover together all the table; or one might consider the maximal radius $R(m)$ of the ball containing no points of this subset (see Figure 3.2).

Let us compare the values $r(m)$ and $R(m)$ calculated from the field tables with the similar characteristics of m genuinely random points: *the field table chaoticity conjecture* claims that these quantities should exhibit similar behaviour for fields of $z = p^n$ elements, where $p \to \infty$ or $z \to \infty$, provided that $m \approx \vartheta z$, where $0 < \vartheta < 1$ is fixed.

Yet another randomness characterisation of a set of m points of the table is the *percolation radius*, defined as follows.

Enclose each point of the set in a ball of radius r, centred at that point. If r is sufficiently small, one cannot cross the table from one side to the opposite

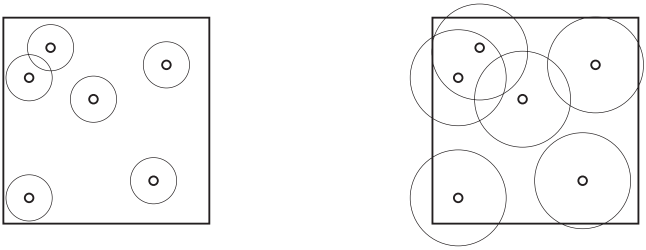


Figure 3.3 Percolation due to the growth in the size of defects

(thus creating an uncontractible path on the torus) along the union of these small balls. If the radius is sufficiently large, then such a ‘percolation’ through the union of the balls, which could be interpreted as defects in a material, becomes possible – see Figure 3.3. (Incidentally, the word ‘percolation’ is borrowed from the study of leaks through the walls of containers.)

The critical (minimal) value $r(m)$ at which the percolation first appears is called the *percolation radius* of a given set of m points: it is the smallest size of defects that can produce leakage.

The *percolation chaoticity conjecture* for the points of the geometric progression $\{A^k\}$ in the field table compares the behaviour of the percolation radius $r(m)$ for m independent random points of the table (say, for $m \approx \vartheta z$, where $0 < \vartheta < 1$ is fixed and the field contains a large number $z = p^n$ of elements).

Note that now, as above, when I mention limiting behaviour I shall mean as $p \to \infty$, but the $z \to \infty$ limit may also be considered.

When studying percolation, it may also be interesting to replace balls of radius r by segments of the progression

$$\{A^k : |k - k_0| \le \varrho\} ,$$

comparing it with a similar set of segments of a random sequence $\{A_k\}$ of m points of the field table. Defining in this way the *quasi-percolation radii* $\varrho(m)$, their conjectured behaviours should be similar for the first $m \approx \vartheta z$ points $\{A^k\}$ of the $z = p^n$ elements of the table of the field and for the random sequence of m points of the table (where, as usual, $0 < \vartheta < 1$ is fixed and $p \to \infty$, or alternatively, $z \to \infty$).

Of course, one is able to invent many different criteria for chaoticity of the tables, and every one of them leads to an (interesting?) conjecture of ergodic character that deserves to be studied empirically (and which would, if the numerical experiments confirm it, later become a proved theorem).

The resulting theory is some number-theoretic finite version of the ergodic theory of toric automorphisms where the chaoticity and the mixing properties of the progressions $\{A^k\}$ have been studied for volume-preserving automorphisms A of the continuous torus T^n.

The distinctiveness of our case depends on the fact that the finite torus $\mathbb{Z}_p^n$ consists of a finite number of points, and that, instead of the infinite time limit used in ergodic theory to define the time average, we let grow the number $m \approx \vartheta z$ of points in the orbit of the dynamical system that we are studying. (This growth can be due to increasing either the parameter p or the number $z = p^n$ of points of the finite torus.)

It is surprising that the percolation chaoticity problem has not been studied, as far as I know, even in the (simpler) case of the ergodic theory of continuous toric hyperbolic automorphisms.

4

Equipartition of geometric progressions along a finite one-dimensional torus

Two very different ways of formulating a problem exist: the *abstract way*, characteristic of Bourbaki, consists of the most general formulation, thus leaving no possibility for further generalisations; and the opposite *concrete way* is *to choose a simple case that cannot be simplified further* yet preserves some content of the problem[†].

I tried in Chapter 3 to formulate the field table randomness conjectures in the abstract form.

Let us consider now the concrete form of the first of these conjectures concerning the equidistribution of progressions in fields of p^n elements. To do it, we restrict ourselves to the simplest field $\mathbb{Z}_p$, which consists of the p residues after division by a prime number p: that is, consider the simplest case $n = 1$ of the general theory of Chapter 3.

To simplify the formulas, we shall suppose the prime p to be odd and we shall choose as the domain G of Chapter 3 the first half of the non-zero elements of the field, that is, $\{c : 1 \leq c \leq (p-1)/2\}$, $|G| = (p-1)/2$.

As the segment of the geometric progression of residues we consider its first $m = (p-3)/2$ terms, $\{A^k : 1 \leq k \leq m\}$.

This strange choice for “half” of the progression ($\vartheta \approx 1/2$) is explained by the statement of the little Fermat theorem: $A^{p-1} = 1$, making $A^k = -1$ for $k = (p-1)/2$. Therefore, this term of the progression is not random at all, although randomness may be expected for smaller k: that is, for $k \leq (p-3)/2$.

Calculating these segments of the progressions of residues modulo p for $p = 5, 7, 11$ and 13, we should first find all the primitive elements A for each of these primes, i.e. those for which the smallest period T of the progression

[†] Tchebyshev, who had many friendly relations with French mathematicians, e.g. Liouville, never discussed any mathematics with them in order to avoid adversely affecting his concrete approach with their influence, as he described it, coming home.

takes exactly the Fermat theorem value $T = p - 1$ – for other A, the period T is a smaller divisor of $p - 1$.

These progressions and periods for $p = 5$ are provided by the following table:

A	$\{A^k\}$	T	N	Σ
1	1, 1, 1, 1	1		
2	2, 4, 3, 1	4	1	$2+1+2+1=6$
3	3, 4, 2, 1	4	0	$1+2+1+2=6$
4	4, 1, 4, 1	2		

The primitive elements here are $A = 2$ and $A = 3$; they are shown as bold characters.

The column N represents the number of visits of the segment of the first $m = (p-3)/2$ terms of the progression to the domain G consisting of those residues that do not exceed $(p-1)/2$. For $p = 5$ we obtain $m = 1$, $(p-1)/2 = 2$, and therefore $N(A = 2) = 1$ and $N(A = 3) = 0$.

The column Σ represents the sum of the distances in $\mathbb{Z}_5$ between consecutive members of the progression. (We consider the progression as a cyclic sequence: that is, we also include the distance from the last member of the period to the first one.)

The differences between the observed frequencies and the space average (measuring the error of the equipartition conjecture for the residues of the geometric progression in the space of the non-zero residues) are equal to:

$$A = 2 \ : \quad \frac{N}{m} - \frac{|G|}{z-1} = \frac{1}{1} - \frac{2}{4} = \frac{1}{2} \,,$$
$$A = 3 \ : \quad \frac{N}{m} - \frac{|G|}{z-1} = \frac{0}{1} - \frac{2}{4} = -\frac{1}{2} \,.$$

We observe that in both cases the error in the approximation to an equidistribution has the absolute value $1/2$. Averaging with respect to the choice of the primitive element A, the equipartition criterion is fulfilled exactly:

$$\frac{\overline{N}}{m} = \frac{|G|}{z-1} \,,$$

where

$$\overline{N} = \frac{\sum N(A)}{\text{the number of the primitive elements } A} = \frac{(1+0)}{2} \,.$$

Similar calculations for the prime number $p = 7$ (with $m = 2$, $|G| = 3$, $z = 7$) provide the following answers:

A	$\{A^k\}$	T	N	Σ
1	$1, 1, \dots$	1		
2	$2, 4, 1, \dots$	3		
3	$3, 2, 6, 4, 5, 1, \dots$	6	2	$1 + 3 + 2 + 1 + 3 + 2 = 12$
4	$4, 2, 1, \dots$	3		
5	$5, 4, 6, 2, 3, 1, \dots$	6	0	$1 + 2 + 3 + 1 + 2 + 3 = 12$
6	$6, 1, 6, 1, \dots$	2		

Here, we have used the fact that the distance between the elements 1 and 5 equals 3 in $\mathbb{Z}_7$.

Thus, the mean number of visits of G is equal to $\overline{N} = (2 + 0)/2 = 1$; therefore, $\overline{N}/m = 1/2$. The spatial average also equals

$$\frac{|G|}{z-1} = \frac{3}{6} = \frac{1}{2} .$$

Therefore, as in the $p = 5$ case, the equidistribution criterion is once more fulfilled exactly, averaging with respect to the choice of the primitive element A.

The answers for the case $p = 11$ take the form $z = 11$, $m = 4$, $|G| = 5$, $z - 1 = 10$:

A	$\{A^k\}$	T	N	Σ
1	$1, 1, \dots$	1		
2	$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$	10	3	30
3	$3, 9, 5, 4, 1, \dots$	5		
4	$4, 5, 9, 3, 1, \dots$	5		
5	$5, 3, 4, 9, 1, \dots$	5		
6	$6, 3, 7, 9, 10, 5, 8, 4, 2, 1$	10	1	30
7	$7, 5, 2, 3, 10, 4, 6, 9, 8, 1$	10	3	30
8	$8, 9, 6, 4, 10, 3, 2, 5, 7, 1$	10	1	30
9	$9, 4, 3, 5, 1, \dots$	5		
10	$10, 1, 10, 1, \dots$	2		

We see from this table that the data about the visits provide the values

$$\overline{N} = \frac{3+1+3+1}{4} = 2\,, \qquad \frac{\overline{N}}{m} = \frac{1}{2}$$

and the space average is equal to

$$\frac{|G|}{z-1} = \frac{5}{10} = \frac{1}{2}\,.$$

Thus, the equipartition criterion is fulfilled exactly when averaging over the choice of the primitive element A. Note that the absolute values of the error for the particular choices of A are all equal to $1/4$.

For the case $p = 13$ we have $z = 13$, $m = 5$, $|G| = 6$, $z - 1 = 12$ and the table of progressions takes the form:

A	$\{A^k\}$	T	N	Σ
1	$1, 1, \ldots$	1		
2	$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, \ldots$	12	4	42
3	$3, 9, 1, \ldots$	3		
4	$4, 3, 12, 9, 3, 1, \ldots$	6		
5	$5, 12, 8, 1, \ldots$	4		
6	$6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1, \ldots$	12	2	42
7	$7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1, \ldots$	12	1	42
8	$8, 12, 5, 1, \ldots$	4		
9	$9, 3, 1, \ldots$	3		
10	$10, 9, 12, 3, 4, 1, \ldots$	6		
11	$11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1, \ldots$	12	3	42
12	$12, 1, 12, 1, \ldots$	2		

In this case the number of visits, averaged over the four primitive elements of the field, is

$$\overline{N} = \frac{4+2+1+3}{4} = 2\tfrac{1}{2}\,.$$

Therefore, $\overline{N}/m = 1/2$. The space average also takes the value

$$\frac{|G|}{z-1} = \frac{6}{12} = \frac{1}{2}\,.$$

Thus, for $p = 13$ the equipartition criterion is also fulfilled exactly, when averaging with respect to the choice of the primitive element A. The individual choices ($A = 2, 6, 7, 11$) provide, respectively, the errors

$$(3/10, -1/10, -3/10, 1/10) .$$

These empirical studies lead us to the following conclusion.

Theorem *Taking averages with respect to the choice of the primitive element A, the equipartition criterion for the distribution of the first $m = (p-3)/2$ members of the progression $\{A^k\}$ distributed among the non-zero residues after division by p is exactly fulfilled for the domain*

$$G = \{1 \leq c \leq (p-1)/2 = |G|\}$$

in the field $\mathbb{Z}_p$ (for any odd prime number p).

In other words, for the average number of visits

$$\overline{N} = \frac{\sum N(A)}{(\text{number of the primitive elements } A)} ,$$

we have the "ergodic" value

$$\frac{\overline{N}}{m} = \frac{|G|}{p-1} = \frac{1}{2} .$$

Proof Along with the primitive element A, the inverse residue modulo p, $B = A^{-1}$, is also a primitive element. We need the following result.

Lemma *The following identity holds:*

$$N(A) + N(B) = m .$$

Proof of the Lemma Taking into account the Fermat congruence $A^{p-1} = A^{2m+2} = 1$, we deduce that the two sequences $\{1 \leq k \leq m\}$ and $\{1 \leq \ell \leq m\}$ of the progressions A^k and $B^\ell = A^{p-1-\ell}$ cover with multiplicity 1 the whole progression $\{A^i, 1 \leq i \leq p-1\}$, except its two trivial ('non-random') terms, $A^{p-1} = 1$ and $A^{m+1} = -1$.

Therefore they cover (with multiplicity 1) every element c other than 1 of the domain G, i.e. $\{2, 3, \ldots, m+1\}$. Thus, the sum $N(A) + N(B)$ of the number of visits of either sequence to the domain G equals m, and the Lemma is therefore proved. □

Taking averages over the choices of the primitive element A, the Lemma implies the equality of the mean number $\overline{N}$ of visits to $m = (p-3)/2$. Indeed, the whole set of the primitive residues A consists of α (disjoint) pairs of the form $\{A, B\}$, where $AB = 1$ (as a residue modulo p). Each pair provides the contribution m to the sum $\sum N(A)$, thanks to the Lemma.

Therefore, the whole sum equals αm, whence we find the average number of visits,

$$\overline{N} = \frac{\sum N(A)}{2\alpha} = \frac{m\alpha}{2\alpha} = \frac{m}{2} \, .$$

Thus, $\overline{N}/m = 1/2$, which proves the Theorem. □

The above tables show that in all our examples the variation $\Sigma = \sum \varrho(A^k, A^{k+1})$ of the whole progression of $p-1$ residues, considered as points on the finite circle $\mathbb{Z}_p$, is given by

$$\Sigma = \frac{p^2-1}{4} \, ,$$

independently of the choice of the primitive residue A.

The mean variation $\overline{\Sigma}$ of a random cyclical sequence of $p-1=4$ points of $\mathbb{Z}_5$ can easily be calculated. It suffices to consider the following six sequences, starting with the residue modulo 1:

$$(1,2,3,4)\,,\ (1,2,4,3)\,,\ (1,3,2,4)\,,$$
$$(1,3,4,2)\,,\ (1,4,2,3)\,,\ (1,4,3,2)\,.$$

Their respective variations Σ are equal to $(5, 6, 7, 6, 7, 5)$ (we have used the distance $\varrho(4, 1) = 2$ in $\mathbb{Z}_5$).

Therefore, the mean value $\overline{\Sigma}$ of the variation of a cyclical sequence of four points on the finite circle $\mathbb{Z}_5$ is given by $\overline{\Sigma} = 6$.

Thus, the variation of the cyclical geometrical progressions formed by the powers of the primitive residues A (after division by $p=5$), calculated above, is given by $\Sigma(A) = 6$; this value coincides with the mean variation $\overline{\Sigma} = 6$ of a random cyclical sequence (of the same length $p-1=4$) of elements of $\mathbb{Z}_5$.

This observation provides one more argument for the quasi-random property of the table of the field of $p=5$ elements.

As the prime number p increases, the mean variation $\overline{\Sigma}$ of a random sequence of $p-1$ points on the finite circle $\mathbb{Z}_p$ grows like $p^2/4$.

This follows from the following argument.

The distance between two randomly chosen points of this finite circle attains values from 1 to $(p-1)/2$. Its mean value is easily calculated to be close to $p/4$. Therefore, the sum of all such distances between consecutive points of our sequence (there are $p-1$ such distances) grows asymptotically with p as $p^2/4$, with a declining relative error.

Thus, the calculations we have presented concerning the variations Σ of cyclic geometric progressions of length $p-1$ in the field $\mathbb{Z}_p$ (for $p \leq 13$)

confirm once more that the table of the finite field with p elements exhibits quasi-randomness.

Remark on the complexity of logarithms The chaoticity of the distribution of geometric progressions of residues leads to interesting facts and conjectures in complexity theory. If a is a primitive residue modulo p, each non-zero residue x modulo p has the form a^k, and the complexity conjecture is that *to calculate the 'logarithm' k of x is a difficult computational problem.*

To define the *measure of difficulty*, one might classify a function (on a finite set with a finite number of values) according to the 'degree of complexity' of the formula defining this function. In order to see how to define a numerical measure of complexity, let us consider the simplest case of the binary functions $f : (\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/2\mathbb{Z})$.

Such a function can be considered as a sequence $(x_1, \dots, x_n)$ of n elements, each of them being either 0 or 1. There are 2^n such sequences, and they form the modulo 2 vector space $(\mathbb{Z}_2)^n$. One can consider these functions as the vertices of a cube of dimension n.

To measure the complexity of a function x following Newton's idea, we associate to it the *first difference function*, y, defined as the sequence of the binary residues

$$y(k) = x(k+1) - x(k) \pmod 2 .$$

Since the argument k is a residue modulo n, we get n differences of n residues, where we take as the element succeeding the final one to be the starting element of the sequence. By making the sequence cyclic, we avoid boundary effects.

Thus, if $x = (1, 0, 0, 1, 1)$, we obtain the differences $y = (1, 0, 1, 0, 0)$, since $y(5) = x(1) - x(5) = 0$.

The difference operator is a linear operator (i.e. an abelian group homomorphism):

$$D : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n .$$

The complexity of a point $x \in \mathbb{Z}_2^n$ will be calculated in terms of the sequence of the consecutive differences,

$$D^t(x) \in \mathbb{Z}_2^n \quad (t = 1, 2, \dots) .$$

Examples *For the constant function x we get $D(x) = D^t(x) = 0$.*

For a polynomial x of degree d, i.e. for $x(k) = a_0k^d + \cdots + a_d$, we get $D^t x = 0$ for any $t > d$.

We shall study below the spectral properties of the linear operator D.

It is natural to consider the constants to be the simplest functions, and polynomials of low degree to be less complicated than those of higher degree, and non-polynomial functions to be even more complicated objects. I shall not formulate the obvious next steps, involving exponentials and then solutions of differential equations – readers can construct their own hierarchy of more and more complicated functions x according to their needs.

The conjecture is that the *logarithmic functions defined above are complicated*. I shall not prove this conjecture, but I shall show several examples that substantiate it.

Other conjectures claim that *most of the* 2^n *functions forming* $\mathbb{Z}_2^n$ *are like random sequences* (at least asymptotically for $n \to \infty$, and at least for the majority of these functions). I shall not prove it, but the examples discussed below provide complicated functions that behave in numerical experiments in a way similar to random sequences. I hope that this quasi-random behaviour is a general phenomenon rather than a special property of our examples.

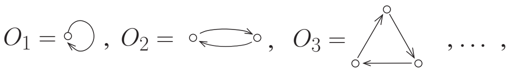
To understand the range of complexity, we start from a general study of the difference operator $D : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$.

Since the operator D is a mapping of a finite set to itself, it decomposes the set $\mathbb{Z}_2^n$ into connected invariant components.

We consider these components as directed graphs, with the edge leaving x connecting the point x with Dx.

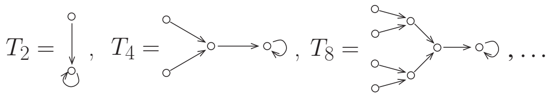
Each connected component of the graph of a mapping consists of:

an attracting cycle O_m of some length $m \geq 1$:

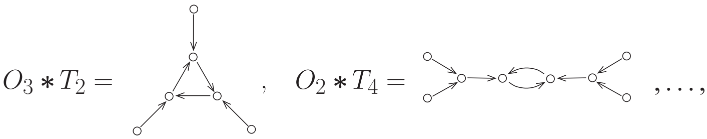


and trees attracted by the vertices of the cycle.

We shall need the binary trees T_{2^q} of 2^q vertices:



We shall denote by $O_m * T_{2^q}$ the component whose cycle O_m attracts a tree T_{2^q} at each vertex: thus, $O_1 * T_{2^q} = T_{2^q}$, and succeeding 'products' are



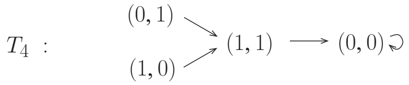
Theorem 4.1 *The graph of the difference operator* $D : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ *has, for* $n \leq 12$, *the form presented in the following table:*

n	number of components	cycles and trees	$D^u = D^v$
2	1	$(O_1 * T_4)$	$D^2 = 0$
3	2	$(O_3 * T_2) + (O_1 * T_2)$	$D^4 = D$
4	1	$(O_1 * T_{16})$	$D^4 = 0$
5	2	$(O_{15} * T_2) + (O_1 * T_2)$	$D^{16} = D$
6	4	$2(O_6 * T_4) + (O_3 * T_4) + (O_1 * T_4)$	$D^8 = D^2$
7	10	$9(O_7 * T_2) + (O_1 * T_2)$	$D^8 = D$
8	1	$(O_1 * T_{256})$	$D^8 = 0$
9	6	$4(O_{63} * T_2) + (O_3 * T_2) + (O_1 * T_2)$	$D^{64} = D$
10	10	$8(O_{30} * T_4) + (O_{15} * T_4) + (O_1 * T_4)$	$D^{32} = D^2$
11	4	$3(O_{341} * T_2) + (O_1 * T_2)$	$D^{342} = D$
12	24	$20(O_{12} * T_{16}) + 2(O_6 * T_{16})$ $+(O_3 * T_{16}) + (O_1 * T_{16})$	$D^{16} = D^4$

The proof is by direct verification. So, for $n = 2$ there are $2^n = 4$ vertices, and the difference operator, by definition, acts as follows:

$$D(0,0) = (0,0)\ ,\ \ D(0,1) = (1,1)\ ,$$
$$D(1,0) = (1,1)\ ,\ \ D(1,1) = (0,0)\ .$$

This gives the graph whose only component is



(4.1)

Denoting by δ the shift operator $(\delta x)_k := x_{k+1}$, we obtain the formulas $D = 1 + \delta$ and $\delta^n = 1$. Therefore we get, for $n = 3$,

$$D = 1 + \delta\ ,\ \ D^2 = 1 + 2\delta + \delta^2 = 1 + \delta^2\ ,\ \ D^3 = 1 + \delta + \delta^2 + \delta^3 = \delta + \delta^2$$
$$D^4 = \delta + \delta^2 + \delta^2 + \delta^3 = \delta + 1 = D\ .$$

Several obvious properties of the formulas in the table can easily be proved in the general situation. Thus, for $n = 2^m$ one has $D^n = 0$, since all the binomial coefficients C_n^i are even for $i \neq 0, n$:

$$D^n = 1 + \delta^n = 1 + 1 = 0 \pmod 2\ .$$

Now we shall study the positions of the logarithmic functions in this table. Explicit calculations show that their complexities are close to the maximal possible value of a binary function, for a given value of n.

For a primitive residue a modulo p, we define the 'logarithm of the residue k' by the Fermat formula

$$a^{\log_a(k)} = k \pmod{p} .$$

Reducing this integer modulo 2, we construct the binary function with the values

$$x(k) = \log_a(k) \pmod{2} \in \mathbb{Z}/(2\mathbb{Z}) \ :$$

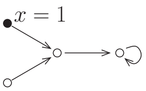
with the arguments taking the values $k = 1, 2, \ldots, p-1$.

Example *The case* $p = 7$*,* $a = 3$ *yields* $\log_3 k = (0, 2, 1, 4, 5, 3)$*,* $x(k) = (0, 0, 1, 0, 1, 1)$.

Thus, we obtain for each a the sequence of $n = p - 1$ logarithms reduced modulo 2, $x \in \mathbb{Z}_2^n$. Now we shall apply the complexity hierarchy defined by the graphs of Theorem 4.1 to this binary sequence x.

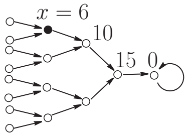
Theorem 4.2 *The modulo* 2 *reduced logarithms* x *of consecutive residues modulo* p *have the following values* (*for* $p \leq 13$) *in terms of the difference graphs of Theorem* 4.1 *for* $n = p - 1$*:*

$p = 3$



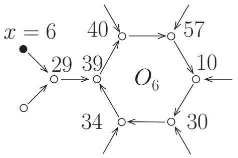
$(x \in T_4 \ , \ a = 2);$

$p = 5$

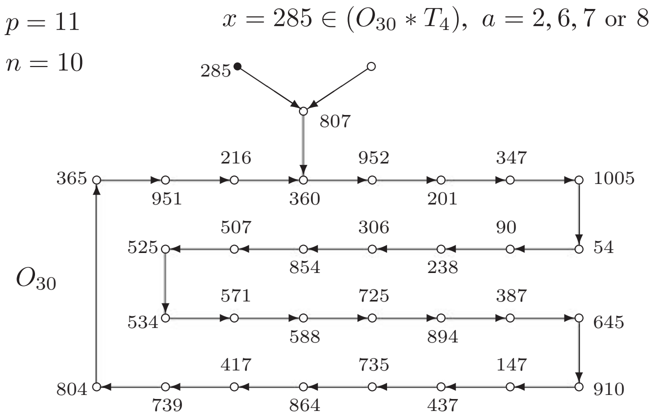


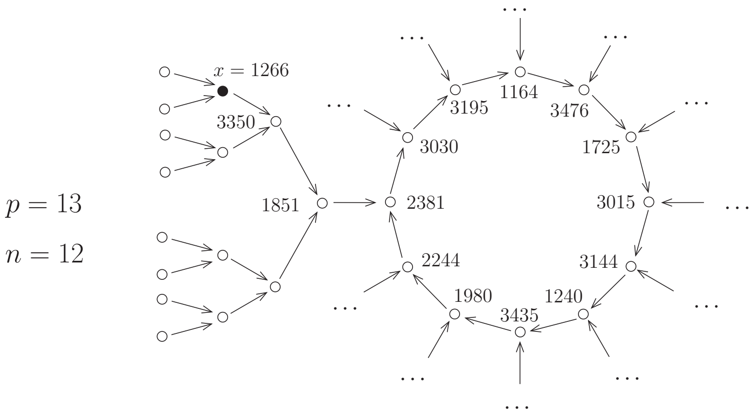
$(x \in T_8 \ , \ a = 2 \text{ or } 3);$

$p = 7$



$(x \in T_{16} \ , \ a = 3 \text{ or } 5);$





$$(x = 1206 \in (O_{12} * T_{16}),\ a = 2, \text{ or } 6, \text{ or } 7, \text{ or } 11);$$

In this description we denote the binary sequence

$$x = (x_1, \dots, x_n) \in \mathbb{Z}_2^n$$

by the ‘binary decimal’ integer

$$2^{n-1}x_1 + 2^{n-2}x_2 + \cdots + x_n \ :$$

thus, $x = 285$ in the case $p = 11$ (and $n = 10$) means the sequence

$$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$$

of the 10 binary digits of the number $285 = 256 + 16 + 8 + 4 + 1$.

The proofs of the statements of Theorem 4.2 involve finite, but long, calculations. In the simplest case, $p = 3$, $a = 2$, the geometric progression $\{2^k\} = 1, 2 \pmod 3$ for $k = 1, 2$ implies the logarithms

$$\log_2 1 = 0 , \quad \log_2 2 = 1 .$$

The sequence of reduced logarithms is $(x_1 = 0, x_2 = 1)$, giving the position of x in the graph of the theorem, according to formula 4.1.

The cases $p = 11$ and 13 show that as the values of p increase, so the calculations become longer. To speed up the calculation, we can reduce the cyclic sequences x of length n modulo the group $\mathbb{Z}/(n\mathbb{Z})$ of n cyclic rotations, identifying, say, the sequences (0100) and (0001) for $n = 4$. For this reduction by the action of δ, it is useful to consider x as a residue modulo $2^n - 1$. Since the operator D commutes with these rotations, this reduction accelerates the calculations (about n fold).

It is also useful to calculate first the kernel of D^t for large t. This kernel is represented by the vertices forming a binary tree.

To obtain the attracted trees of the cycles it is sufficient to add this subspace of $\mathbb{Z}_2^n$ to the points of the cycle. This reasoning explains the homogeneity of the graphs in the table of Theorem 4.1: all the attracted trees are isomorphic to the above kernel (since the union of the cycles is the image of the linear operator D^t for large t).

These long calculations lead to the table in Theorem 4.2, which, by comparison with that in Theorem 4.1, shows that the complexity of the logarithmic function almost attains the maximal possible value for any binary function on a set of n points.

This observation follows from both theorems only in the case $n \leq 12$, but it may be worth investigating for larger values of n, at least as a plausible conjecture.

Similar theorems and conjectures can also be contemplated for the non-binary functions, for instance, for those functions whose values are residues modulo some integer q:

$$x \in (\mathbb{Z}/q\mathbb{Z})^n , \quad x_k \in \mathbb{Z}_q .$$

Unfortunately, I cannot begin to guess the answers to such a generalisation of Theorem 4.1, even for $q = 2$, as above: the table of Theorem 4.1 shows a rather irregular dependence on n, and even the averaged asymptotics for $n \to \infty$ are interesting, but undecipherable.

All these theorems and conjectures can be extended to general Galois fields almost by inspection, but I have restricted myself above to the simplest case of the field $\mathbb{Z}_p$ of residues and sometimes only to the binary base $\mathbb{Z}_2$, since, in order to understand the (unknown) complexity theory, we should start from the simplest cases.

The author is grateful to Prof. Shparlinski (Department of Computing, Macquarie University, Sydney), who, after reading the original draft of the present book, proved some of the conjectures discussed above, and also corrected some misprints in my earlier publications.

5

Adiabatic study of the distribution of geometric progressions of residues

I shall describe here some physical arguments that shed light on the asymptotic equipartition, as p tends to infinity, of the sequence of the residues modulo p of the members of the geometric progression

$$\{A^k, 1 \leq k \leq \vartheta p\}$$

among all the non-zero residues modulo p, where A is a primitive residue and the number ϑ, $0 < \vartheta < 1$, is fixed.

We shall try to evaluate the number N of those residues c from the members of the progression whose value lies in the interval

$$G \ : \quad 1 \leq c \leq \mu p \ .$$

To estimate N we shall use logarithms, thereby transforming the geometric progression into an arithmetic one:

$$\ln A^k = \ell_k = ka \qquad \text{(where } a = \ln A\text{);}$$

here, logarithms make sense as real numbers.

The condition $A^k (\text{mod } p) \in G$ can be written in terms of logarithms as the inclusion of the number ℓ_k into one of the intervals of the following system (represented in Figure 5.1):

$$\ell_k \in \bigcup \Delta_j ,$$

where Δ_j is the gap between the logarithms of members of two arithmetic progressions:

$$\Delta_j = \{\ell : \ln(jp) < \ell \leq \ln(jp + \mu p)\} \ .$$

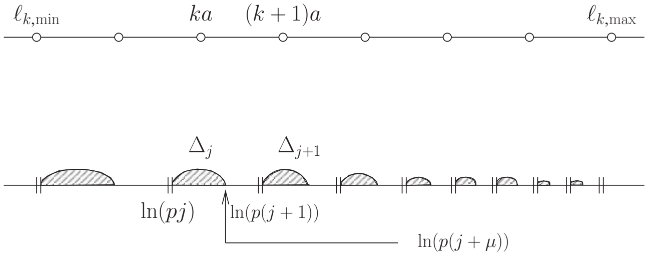


Figure 5.1 Adiabatic approximation of a non-uniform sequence of logarithms of members of an arithmetic progression

The length of the gap Δ_j equals

$$|\Delta_j| = \ln \frac{jp+\mu p}{jp} = \ln\left(\frac{j+\mu}{j}\right) = \ln\left(1+\frac{\mu}{j}\right) \approx \frac{\mu}{j}\,,$$

for large j.

The sum $D(\mu)$ of the lengths of all these intervals is a quantity of order $\mu\sum(1/j)$, where the numbers j of the intervals that form this finite sum are fixed by the maximal and minimal logarithms ℓ_k of the members of our geometric progression.

This leads to an approximate relation

$$D(\mu) \sim \mu \ln(j_{\max}) \qquad (\text{where } j_{\max} \to \infty \text{ for } p \to \infty)\,,$$

the word 'approximation' refers here to the size of the relative error.

The total length of the whole interval of the axis ℓ that contains all our logarithms ℓ_k is given by $D(\mu = 1) \sim \ln(j_{\max})$. The arithmetic progression $\{\ell_k\}$ is uniformly distributed along the ℓ-axis, according to H. Weyl's theorem on the equipartition of the fractional parts of an arithmetic progression in the interval (0, 1).

This leads to our guessing that the number N of visits of the points ℓ_k to the union of the intervals Δ_j should be asymptotically proportional to the fraction formed by the sum of the lengths of these intervals in the length of the whole segment of the axis ℓ. That is, it should be asymptotically proportional to the ratio $D(\mu)/D(1)$.

We arrive, therefore, at the conclusion that, for $p \to \infty$, one should expect the asymptotic behaviour of the number of visits to be

$$\frac{N}{\vartheta p} \longrightarrow \left(\frac{D(\mu)}{D(1)} \sim \mu\right)\,,$$

which is the asymptotic equipartition of the sequence of the residues after division by p of the members $\{A^k, 1 \leq k \leq \vartheta p\}$; we counted visits to the domain G, which forms the μth part of $\mathbb{Z}_p$.

Remark 5.1 The next term of the development $\ln(1+x) \approx x - \frac{x^2}{2} + \cdots$ (for small x) leads to the prediction that one should expect the upper limit to decline from the asymptotic value $N > \vartheta\mu(p-1)$.

Remark 5.2 Our reasoning (which is far from mathematically rigorous) may be interpreted as some kind of adiabatic replacement of the logarithmically non-uniform sequence (of the numbers $\ln(jp) = \ln p + \ln j$ and of the intervals Δ_j starting at these points) by the arithmetic progressions (of the respective numbers and intervals) – see Figure 5.1.

In fact, the 'step' $\ln(j+1) - \ln j = \ln \frac{j+1}{j} \sim 1/j$ of the logarithmic sequence decreases slightly as j grows, and therefore this sequence is not exactly an arithmetic progression (though it is rather close to one for rather long intervals of changing j, provided that the step of the approximating arithmetic progression is chosen appropriately to the range of j).

If the logarithmic sequence were an arithmetic progression, our reasoning would be based strictly on Weyl's theorem on the equidistribution of fractional parts.

Thus, the rest of our heuristic reasoning depends on the evaluation of the error in the adiabatic approximation – or, alternatively, on modifying the proof of Weyl's theorem to include the study of the behaviour of the Fourier coefficients of the characteristic function of the union of the intervals Δ_j.

For $p = 997$, $\vartheta = 1/2$, $\mu = 1/2$, $A = 7$, I have calculated the number N of visits to be 279, which is larger than the conjectured asymptotic expression $\vartheta\mu(p-1) \approx 249$.

For $p = 1009$, $A = 11$ and $\vartheta = \mu = 1/2$ the number of visits of the residues 11^k modulo 1009, $1 \leq k \leq 503$, to the domain $G = \{1 \leq x \leq 504\}$ is $N = 269$. The asymptotic expression gives $\vartheta\mu(p-1) \approx 252$, suggesting that the difference between N/m and $|G|/z$ drops off like $c/\sqrt{p}$. It would be interesting to see more examples, for larger p, to evaluate the decline empirically.

The quantities $N(A)/m$ that correspond to different primitive elements A may deviate from the mean for some exceptional values of A, and the evaluation of the dispersion of this deviation might provide some interesting information about how rare are those exceptional values of A for large primes p.

The following construction provides a different approach to the asymptotic equipartition of the sequence of residues modulo p of the members of the geometric progression $\{A^k, 1 \leq k \leq \vartheta p\}$ within all the residues modulo p, where A is a primitive residue and the number ϑ is fixed with $0 < \vartheta < 1$.

Consider the multiplicative group of the complex numbers

$$\mathbb{Z}_p = \{z \in \mathbb{C} : z^p = 1\} .$$

The functions on this group are the (Fourier) linear combinations of the characters

$$e_0 \equiv 1, \quad e_1 = z , \quad e_2 = z^2 , \ \dots , \quad e_{p-1} = z^{p-1} .$$

Multiplication by A of the residues modulo p can be represented using this notation as the mapping $f : \mathbb{Z}_p \to \mathbb{Z}_p$, where $f(x) = x^A$. This mapping acts on the functions as a linear operator (and as an algebraic morphism)

$$f^* e_k = e_{Ak} .$$

The function e_0 is invariant under this mapping, while the remaining $p - 1$ characters are permuted cyclically (here, A is a primitive element).

To prove equipartition one has to prove that the time averages of the functions orthogonal to e_0 converge to zero. For the character e_k, we have to study the time average

$$\widehat{e_k} = \sum_{t=0}^{T-1} \left(f^*\right)^t e_k/T .$$

To study this averaged function, once again take the Fourier transform by ordering the harmonics e_k ($k \neq 0$) as they come in the above cyclic permutation of order $p - 1$; that is, in the order of the sequence of the residues A^t (mod $p - 1$) in $\mathbb{Z}_{p-1}$.

To do it, we consider the multiplicative group of complex numbers,

$$\mathbb{Z}_{p-1} = \{w_t = e^{2\pi i t/(p-1)}\} ,$$

for $0 \leq t < p - 1$. The corresponding harmonics $E_0, \dots, E_{p-2} : \mathbb{Z}_{p-1} \to \mathbb{C}$ are defined by the formula $E_r(w) = w^r$.

As explained above, we identify the characters e_k ($k \neq 0$) with these functions E_r in such a way that the sequence

$$e_1 , f^* e_1 , (f^*)^2 e_1 , \dots , (f^*)^{p-2} e_1$$

takes the form

$$E_0 , E_1 , E_2 , \dots , E_{p-2}$$

and the operator f^* hence takes the form $E_r \to E_{r+1}$ of multiplication by the function w (which is equal to E_1).

For the time average we obtain the expression

$$\widehat{E}_r = \frac{1}{T}(1 + w + w^2 + \cdots + w^{T-1})E_r = \frac{1}{T}\,\frac{w^T - 1}{w - 1}E_r\ ,$$

which tends to zero for large T and for any value of r and, hence, for all the characters e_k, $k \neq 0$.

Thus, *the time average of any function on the group $\mathbb{Z}_{p-1}$ tends to its space average for $T \to \infty$.*

The space average of the harmonic e_k along $\mathbb{Z}_{p-1}$ is easy to compute:

$$\frac{1}{p-1}\sum_{t=0}^{p-1}\left((f^*)^t e_k\right) = \frac{1}{p-1}\sum_{k=1}^{p-1} e_k = -\frac{e_0}{p-1}\ ,$$

since $\sum_{k=0}^{p-1} e_k = 0$, by Vieta's theorem for the equation $z^p = 1$.

Therefore, the mean value $\widehat{e_k}$ tends to 0 as $p \to \infty$ if $k \neq 0$.

Thus, the time average along the segment of the geometric progression $\{A^t\}$ of any fixed linear combination of the harmonics on the group $\mathbb{Z}_p$ tends to its space average as $p \to \infty$.

Applying this to the characteristic function of the part G of the group $\mathbb{Z}_p$, we obtain a proof of the claim about the asymptotic equipartition for the segment of the progression at the limit $p \to \infty$.

This reasoning is, however, inadequate for a rigorous proof, since the characteristic function of the domain G is not a fixed linear combination of the harmonics: the number of the harmonic summands that are needed to approximate this characteristic function of G on $\mathbb{Z}_p$ grows with p.

Remark In our study of the asymptotic equipartition as $p \to \infty$ we have fixed the (Jordan measurable) domain G in the real continuous torus T^n, evaluating the number N of visits of a sequence $\{A^k\}$ to the corresponding domain $G(p)$ of the finite n-torus $\mathbb{Z}_p^n$; this domain consists of a finite number of points (growing with p).

Perhaps, together with the natural domains G (similar to the band $0 \leq u \leq d$ in T^2), one could take also some more complicated domains $G(p)$ – similar, say, to the set defined by the condition that u is even for the points $(u, v) \in \mathbb{Z}_p^2$.

The conjecture then becomes *that asymptotic equipartition holds as $p \to \infty$ even for such 'irregular domains', provided that the algorithm defining the domain $G(p)$ is sufficiently simple.*

I do not know any proved theorem of this kind (which would be interesting even for the distribution of the fractional parts of members an arithmetic progression on a circle), though the Skolem theorem on the zeroes of recurrent sequences $\{a_k\}$ could be considered as some sort of confirmation of this conjecture. Skolem's theorem claims that *the set* $\{t : a_t = 0\}$ *consists of a finite set of arithmetic progressions of integers* t, *whatever the recurrent sequence might be*.

The ergodic theory content of the conjectured chaoticity theorems is the statement that *sufficiently chaotic dynamics reduces the predictability of all those properties of the trajectories that can be computed by simple algorithms*.

Remark The study of the equipartition of finite segments of geometric progressions along 'irregular' domains of the one-dimensional finite torus $\mathbb{Z}_p$, as described above, might be useful for the investigation of the degree of equipartition of segments of geometric progressions in finite fields with a large number $z = p^n$ of elements, living on an n-dimensional torus.

The point is that the mapping $k \mapsto A^k$ bijectively sends the set of non-zero residues modulo $z - 1$ to the set of non-zero elements of a field of z elements (living on an n-torus).

Therefore, if we know the equipartition property for the *arithmetic* progression $\{t \cdot r, \text{ with } t = 1, 2, 3, \dots\}$ on the 1-dimensional finite torus $\mathbb{Z}_{z-1}$, then we can deduce information about the partition of the geometric progression $\{B^t, \ t = 1, 2, 3, \dots\}$, where $B = A^r$, along the finite n-torus $\mathbb{Z}_p^n$ (consisting of $z = p^n$ points).

For instance, to study the asymptotic behaviour of the number N of visits of a segment of a geometric progression $\{B^t\}$ to a domain G of a field of z elements, it would suffice to know the asymptotic behaviour of the number of visits of the corresponding segment of an arithmetic progression $\{t \cdot r, \ t = 1, 2, 3, \dots\}$ to the full pre-image $f^{-1}G$ of the domain G under the above bijection $k \mapsto A^k$, which we have denoted by f.

In this sense, in order to prove the asymptotic equipartition of the segments $\{B^t\}$ of a geometric progression along the n-dimensional finite torus, it would be enough to prove that the number of visits to subdomains of the finite circle $\mathbb{Z}_{z-1}$ by the segment $\{t \cdot r\}$ of the arithmetic progression is proportional to the measure of the subdomain. But one needs to know this inequality of approximate proportionality for subdomains (different from the ordinary intervals) of the finite circle, provided that the subdomain is defined by an algorithm of bounded complexity (like, say, the domain $f^{-1}(G)$ for the domain G that we have been studying on the finite torus).

Although arithmetic progressions are much simpler objects to study than geometric ones, as far as equipartition is concerned, what we know about them is insufficient for two reasons: one needs to study visits to complicated domains

$f^{-1}(G)$, and the number $z - 1 = p^n - 1$ of points of the one-dimensional finite torus $\mathbb{Z}_{z-1}$ is not prime.

Despite the formal inadequacy of equipartition results on finite circles, in relation to our problem, it seems that it might not be too difficult to obtain the relevant results about the equipartition of arithmetic progressions that are needed to study the equipartition of geometric progressions along n-tori.

6
Projective structures generated by a Galois field

The algebra of a Galois field has a remarkable geometrical aspect that is similar to the projective geometry view of linear algebra in, for example, the use of the geometry of the principal axes of ellipsoids and hyperboloids instead of the theory of eigenvalues of quadratic forms. Calculations are usually simpler in the algebraic version, but real understanding is reached only by the geometric approach to the theory of principal axes.[†]

I shall describe now the geometric version of the algebra of a Galois field: the theory of projective structures on finite sets and the study of the action on them of the groups of 'Frobenius transformations'

$$\Phi_k(x) = x^k \ ,$$

i.e. of calculation of powers. We recall first some notation concerning the projective line. Consider *all the straight lines containing the point* 0 *of the usual plane* $\mathbb{R}^2$. The manifold of all such lines is one-dimensional and is diffeomorphic to the circle.

To see this, describe the points of the plane by their Cartesian coordinates (u, v). The line is then described by its equation $u = \lambda v$, where λ is a constant that is determined by the chosen line (see Figure 6.1).

The constant λ is called *the affine coordinate on the projective line* (whose points are the straight lines of the plane going through the origin 0).

However, just as the whole sphere cannot be represented by a continuous map on a plane, the values of the affine coordinate λ do not describe all the straight lines going through the origin. In particular, they do not describe the vertical line (given by $v = 0$ in Figure 6.1). Therefore, one adds an 'infinite' point $\lambda = \infty$ to the axis of the variable λ, providing the description of the

[†] Goethe said that 'Mathematicians are like Frenchmen: whatever you say to them they translate into their own language and forthwith it is something entirely different.'

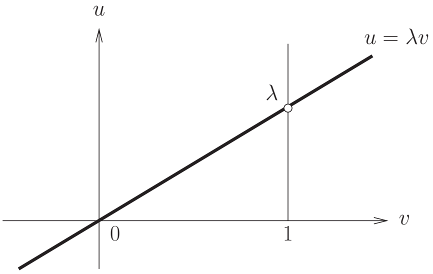


Figure 6.1 A projective line and its affine coordinate λ

whole real projective line $\mathbb{R}P^1$ by the values

$$\mathbb{R}P^1 \sim \{\lambda \in \mathbb{R}\} \sqcup \{\lambda = \infty\} ,$$

where the symbol $\sqcup$ means 'disjoint union'.

This point at infinity, $\lambda = \infty$, of the projective line (representing the vertical line $v = 0$ in Figure 6.1) is as valid as all the others, since the vertical line on the plane is as valid as the others: for example, any line through the origin can be transformed to any other such line by a rotation in the plane.

A different choice of the initial coordinate system on the plane (one can take, say, $\tilde{u} = v$, $\tilde{v} = u$) would produce a different affine coordinate $\tilde{\lambda}$ (in our example, $\tilde{\lambda} = \tilde{u}/\tilde{v}$) and a different point $\tilde{\lambda} = \infty$ on the projective line $\mathbb{R}P^1$ (which would correspond in our example to the horizontal line $\tilde{v} = 0$ in Figure 6.1).

In the neighbourhood of the vertical line shown in Figure 6.1, where $\tilde{\lambda} = 0$ in our example, the new affine coordinate $\tilde{\lambda}$ ($\tilde{\lambda} = 1/\lambda$ in our example) is a regular parametrisation of the real projective line. Therefore, whether the affine coordinate λ tends to $+\infty$ or $-\infty$, we are led to the same place ($\tilde{\lambda} = 0$) of the manifold of the straight lines containing the origin of the plane.

This compact manifold, the *real projective line*, is therefore diffeomorphic to the circle (see Figure 6.2):

$$\mathbb{R}P^1 \approx S^1 .$$

For a different choice of linear coordinates (which can be non-orthogonal) on the plane, the new affine coordinate $\tilde{\lambda}$ would be a fractional-linear function of the old one:

$$\tilde{\lambda} = \frac{a\lambda + b}{c\lambda + d} , \tag{6.1}$$

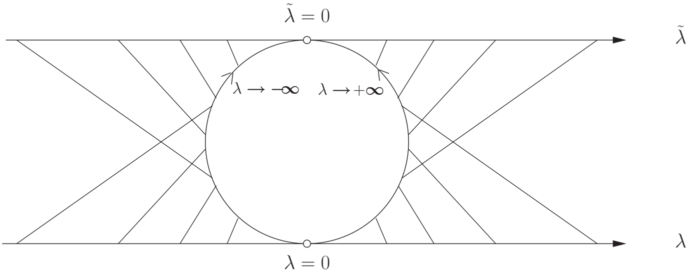


Figure 6.2 The real projective line diffeomorphism to a circle

since the new coordinates have the form

$$\tilde{u} = au + bv \ , \quad \tilde{v} = cu + dv \ .$$

The new coordinate axes should not coincide, which means $ad \neq bc$.

The transformation of the λ-axis that is defined by the formula (6.1) is called a *projective transformation*. The λ-axis is considered here as being completed by the point at infinity, and the formula (6.1) defines a diffeomorphism of the real projective line (that is, of a circle) onto itself.

Of course, the algebraic versions of this simple geometry are the conventions

$$\tilde{\lambda} = \infty \quad \text{for } c\lambda + d = 0 \ , \quad \tilde{\lambda} = a/c \quad \text{for } \lambda = \infty \ .$$

The real $(n-1)$-dimensional projective space,

$$\mathbb{R}P^{n-1} = (\mathbb{R}^n \setminus 0)/(\mathbb{R} \setminus 0) \ ,$$

is defined similarly to the projective line: it is the manifold of all straight lines going through the origin 0 of the n-dimensional vector space $\mathbb{R}^n$.[†]

Its affine chart is constructed from a linear coordinate system $(u_1, \ldots, u_n)$ in $\mathbb{R}^n$: if $u_n \neq 0$, we define the vector $\lambda \in \mathbb{R}^{n-1}$, whose coordinates are

$$\lambda_1 = u_1/u_n \ , \ldots \ , \quad \lambda_{n-1} = u_{n-1}/u_n \ .$$

In other words, we take the point of intersection, λ, of the line that we wish to describe with the hyperplane $u_n = 1$ of $\mathbb{R}^n$: this point is the image of the line on the affine chart $\mathbb{R}^{n-1}$ – similar to the situation of Figure 6.1 where $n = 2$.

To obtain all the straight lines through the origin of $\mathbb{R}^n$, one has to use n such affine charts, represented by the n hyperplanes, $\{u_n = 1\}, \ldots, \{u_1 = 1\}$. Thus for $n = 2$ one needs two charts, λ and $\tilde{\lambda}$ in Figure 6.2.

[†] Goethe described this definition of the projective space, including its ‘infinitely far points’, by the words ‘Willst du ins Unendliche schreiten, geh nur im Endlichen nach allen Seiten’: ‘you want to reach infinity, move in the finite domain in all directions.’

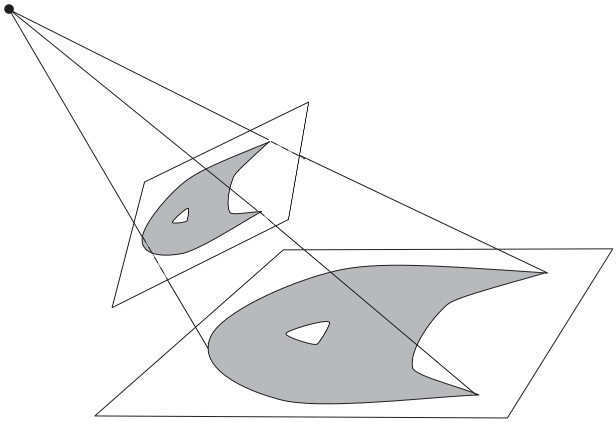


Figure 6.3 A projective transformation of a cat

The corresponding fractional-linear transformations are described in $\mathbb{R}P^m$ by the following extension of formula (6.1): for $j = 1, \ldots, m$, the coordinates of the image point of the point λ that has affine coordinates $(\lambda_1, \ldots, \lambda_m)$, are

$$\tilde{\lambda}_j = \frac{a_{j,1}\lambda_1 + \cdots + a_{j,m}\lambda_m}{b_1\lambda_1 + \cdots + b_m\lambda_m} \, ;$$

it is important to observe that the denominator is independent of the number j of the coordinate $\tilde{\lambda}_j$.

The geometric meaning of these algebraic formulas is that they describe the projective transformations that are obtained (say, for $m = 2$) when we project one plane P in 3-space onto another plane $\tilde{P}$, by rays that start at a common projection centre (see Figure 6.3).

So, the theory that we are describing is basic both for the geometry of the projections that send straight lines to straight lines, and to the theory of perspective (where the parallel rails of a straight railway ‘meet at an infinitely far point on the horizon’).

The great Italian painter Paolo Uccello (whose name means ‘Bird’) was one of the first painters to make a serious study of the mathematical theory of perspective. It is said that when his wife once invited him at midnight to her chamber, he replied ‘I am coming – what a nice perspective’, though what he had in mind was the beauty of his remarkable drawing.

To become familiar with projective geometry, the reader may try to prove the following facts:

(i) *The real projective plane is non-orientable*; the real projective space $\mathbb{R}P^m$ is orientable if the dimension m is odd and non-orientable for even m.

(ii) The complement of a small disc on the real projective plane is diffeomorphic to the *Möbius band* (it was because of this fact that Möbius discovered this surface).

The complex projective space $\mathbb{C}P^m$ is defined similarly to the real one, but starting from the complex vector space $\mathbb{C}^n$, where n is still equal to $m + 1$. The points of this complex projective space are the complex straight lines going through the origin of $\mathbb{C}^n$:

$$\mathbb{C}P^{n-1} = (\mathbb{C}^n \setminus 0)/(\mathbb{C} \setminus 0) .$$

Affine coordinates and projective transformations are defined by the same formulas as in the real case[†].

In the case of complex projective spaces and transformations, the difficulties (i) and (ii) described above vanish. Thus, the complex projective line, $\mathbb{C}P^1$, can be obtained from the λ-axis of the complex plane by the addition of a point at infinity. The resulting variety is diffeomorphic to the ordinary sphere S^2 and is called the *Riemann sphere*.

In the neighbourhood of the point at infinity, $\lambda = \infty$, the affine complex coordinate is the function $\tilde{\lambda} = 1/\lambda$.

The hypersphere in $\mathbb{C}^n$ that is defined by the equation

$$\sum |u_k|^2 = 1$$

is diffeomorphic to the hypersphere S^{2n-1} of the real vector space $\mathbb{R}^{2n}$. This hypersphere is intersected by the complex straight lines that go through the origin 0 of the complex space $\mathbb{C}^n$ along real circles S^1.

The real lines of $\mathbb{R}^n$ that go through zero intersect the hypersphere S^{n-1} ($\sum |u_k|^2 = 1$) along 0-dimensional spheres S^0 (each of which consists of two opposite points).

Whereas the real projective space $\mathbb{R}P^m$ can be obtained from the sphere S^m by gluing together all pairs of opposite points that are proportional vectors of the real vector space, i.e.

$$\mathbb{R}P^m = S^m/(S^0 = \{\pm 1\}) ,$$

we obtain *the complex projective space*, $\mathbb{C}P^m$, from the sphere S^{2n-1} (where $n = m + 1$) by identifying with a point each circle S^1 along which the sphere intersects a complex straight line that goes through the origin.

[†] This is the important advantage of algebra: some people are happy to apply their formulas to objects that are quite different from those for which these formulas have been proved, and if the result happens to be wrong, they postulate it to be presumably true for ‘ideal’ objects, thereby replacing the difficult study of the real world by the easier investigation of ‘ideal’ objects.

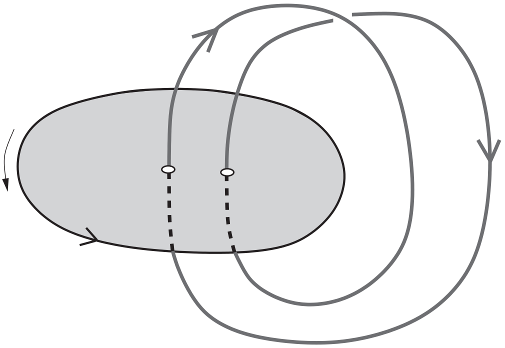


Figure 6.4 Two curves having a linking number equal to 2

All the points of this circle are complex proportional vectors of the complex vector space, and they can be obtained from an arbitrary point of this circle by multiplying it by all the complex numbers of modulus 1:

$$\mathbb{C}P^m = S^{2m+1}/(S^1 = \{e^{i\varphi}\}) .$$

The truly 4-dimensional manifold $\mathbb{C}P^2$ can be obtained from the affine complex plane $\mathbb{C}^2$ by the addition 'at infinity' of a complex projective line $\mathbb{C}P^1$; that is, of a Riemann sphere:

$$\mathbb{C}P^2 = \mathbb{C}^2 \cup S^2 .$$

The complex projective line $\mathbb{C}P^1$ can also be described as the manifold whose points are the special great circles S^1 of S^3. A special great circle means the intersection of the 3-sphere S^3 with a complex straight line of $\mathbb{C}^2$ that contains the origin 0. In other words, a special great circle is the set of points of the sphere S^3 that are complex proportional to a given point. So the space of special great circles is:

$$\mathbb{C}P^1 = S^3/(S^1 = \{e^{i\varphi}\}) .$$

It is interesting to note that different special great circles in the 3-dimensional sphere S^3, which is fibred into these circles, have special locations in the sphere: the linking number of any pair of such special great circles is equal to 1.

The *linking number* of two disjoint oriented smooth closed curves in the oriented 3-sphere (or in the oriented Euclidean 3-space) is defined as the intersection index of one of these circles with any smooth oriented immersed compact surface whose boundary is the other circle (see Figure 6.4).

The orientations are used here in the following way: the orienting frame of the surface at a boundary point consists of the orienting vector of the boundary curve, followed by the tangent vector to the surface, directed internally.

The *intersection index* of the second curve with the surface whose bound is the first curve, is found by counting the intersection points of these two objects, equipped with their signs which are positive if the 3-frame formed by the three vectors orienting the curve and the surface orients positively the 3-space.

The linking number of two curves does not depend on the choice of the surface bounded by one of the curves: the surface should only be nowhere-tangent to the second curve. The linking number L of two oriented curves is symmetric with respect to their ordering: $L(\mathrm{I}, \mathrm{II}) = L(\mathrm{II}, \mathrm{I})$.

The fibration of the 3-sphere whose fibres are the above special great circles is called the *Hopf fibration*, $S^3 \to (\mathbb{C}P^1 = S^2)$: its fibre is S^1. This fibration is a basic object in many branches of mathematics.

The 3-sphere S^3 is the ordinary Euclidean 3-space compactified by the addition of one point. In this model of the 3-sphere, the Hopf fibration becomes the decomposition of the Euclidean 3-space into a straight line (originating from the circle containing the added point) and the complement to this line, fibred into closed curves whose pairwise linking numbers are all equal to 1.

Although I can draw the resulting nice picture, I shall not do so here, but leave to the readers the pleasure of drawing it for themselves.

Instead, we shall now transfer the theory described above in the real, and in the complex, case, to the situation in which the numbers are replaced by the residues modulo a prime p: we shall define the *finite projective spaces* $P^m(\mathbb{Z}_p)$, in a way very similar to that in which we have defined the real manifolds $\mathbb{R}P^m$ and the complex manifolds $\mathbb{C}P^m$, but now consisting of a finite number of points.

We shall start from the finite projective line $P^1(\mathbb{Z}_p)$. It is defined as the set of the straight lines of the finite plane $\mathbb{Z}_p^2$ containing the origin:

$$P^1(\mathbb{Z}_p) = (\mathbb{Z}_p^2 \setminus 0)/(\mathbb{Z}_p \setminus 0) .$$

In terms of the coordinates (u, v) on the finite plane (which are now residues modulo p), the equation of a straight line has the form $u = \lambda v$, but the ‘affine coordinate’ $\lambda \in \mathbb{Z}_p$ is also a residue modulo p.

To obtain all the straight lines, we add to these p values of the affine coordinate λ one more value, denoted by the symbol ∞ (to include the vertical line $v = 0$, taking into account that $\lambda = u/v$ for $v \neq 0$).

Therefore, the finite projective line $P^1(\mathbb{Z}_p)$ consists of $p + 1$ points:

$$|P^1(\mathbb{Z}_p)| = p + 1 \quad (\lambda = 1, 2, \ldots, p; \infty) .$$

The projective transformations

$$\lambda \mapsto \frac{a\lambda + b}{c\lambda + d} \tag{6.2}$$

(where a, b, c and d belong to $\mathbb{Z}_p$, and $ad - bc \neq 0$) permute in some way the $p + 1$ points of the finite projective line, but these permutations are not arbitrary.

Indeed, the symmetric group $S(p + 1)$ of all the permutations of $p + 1$ points of our finite projective line consists of $(p + 1)!$ permutations, and the order of the group of the projective transformations (6.2) is much smaller.

Lemma *The group* $\mathrm{PL}(\mathbb{Z}_p)$ *of the projective transformations* (6.2) *of the finite projective line consisting of* $p + 1$ *points is formed by* $p(p^2 - 1)$ *permutations.*

Proof Indeed, if $a \neq 0$, we can divide all the coefficients by a, to get the transformation (6.2) in a form where $\tilde{a} = 1$. The coefficients, $\tilde{b}$ and $\tilde{c}$, may (independently of each other) each have p values, while the remaining coefficient, $\tilde{d}$, has to satisfy the condition $\tilde{d} \neq \tilde{b}\tilde{c}$ and, for fixed values of $\tilde{b}$ and $\tilde{c}$, can take $p - 1$ possible values. In this way we get $p^2(p - 1)$ transformations (6.2).

In the remaining case $a = 0$, the non-degeneracy condition is $bc \neq 0$. If $d \neq 0$, we can reduce the formula (6.2) to the form where $\tilde{d} = 1$ by dividing by d; the number of such transformations is $(p - 1)^2$, since $\tilde{b}\tilde{c} \neq 0$.

Finally, in the case $a = d = 0$, the transformation has the form $\lambda \mapsto b\lambda$, and the number of such transformations is $p - 1$, since $b \neq 0$.

Thus, the total number of projective transformations of the finite projective line $P^1(\mathbb{Z}_p)$ of all three kinds is equal to the sum

$$p^2(p - 1) + (p - 1)^2 + (p - 1) = (p - 1)(p^2 + (p - 1) + 1) = p(p^2 - 1)\,,$$

proving the Lemma. □

Now, if p is large, then $(p + 1)!$ is much larger than $p(p^2 - 1)$. Indeed, it is so even for $p = 5$, since $(p + 1)! = 720$ and $p(p^2 - 1) = 120$.

I point this out because it shows that *the group of projective permutations of the points of the finite projective line is the small subset* (*of the permutation group* $S(p + 1)$) *formed by those permutations that preserve some remarkable geometric structure in the finite set* $P^1(\mathbb{Z}_p)$ *consisting of* $p + 1$ *points.*

Unfortunately, I have no geometric description of this remarkable structure of the finite projective line, though algebraically this structure is described by an affine coordinate $\lambda \in \mathbb{Z}_p$ of the complement to some 'infinitely far situated' point, $\lambda = \infty$, of a finite set M equipped with a projective structure.

A different coordinate, $\tilde{\lambda} : (M \setminus \bullet) \to \mathbb{Z}_p$, defines the same projective structure on M as does the affine coordinate λ, if it is related to λ by a projective transformation (6.2).

While this algebraic description of the projective structures on a finite set M is not that geometric, it will be used below for the study of those projective structures on sets of $p+1$ elements that are generated by a Galois field of p^2 elements. We shall also use it to study the action of the Frobenius mappings on the projective structures of these finite sets.

Indeed, by fixing a multiplicative generator A for a field of p^2 elements, we can identify bijectively this field with the finite plane (or torus) $\mathbb{Z}_p^2$ of the field table, as was described in Chapter 2.

Consider now the finite projective line $P^1(\mathbb{Z}_p)$ whose $p+1$ points are the $p+1$ straight lines of the finite plane $\mathbb{Z}_p^2$ that contain the origin.

Lemma *The set of straight lines containing the origin of the finite plane $\mathbb{Z}_p^2$, considered as the field of p^2 elements, does not depend on the choice of the multiplicative generator A that was used to identify the field with the finite plane.*

Proof For two proportional points x and cx, where $c = 1 + \cdots + 1$ is a scalar (i.e. two points on the same line in the table), the corresponding elements of the field are also scalar proportional: A^k and $A^k + \cdots + A^k = cA^k$. Since this relation does not depend on the choice of the generator A, the Lemma is proved. □

The set of lines in the finite plane $\mathbb{Z}_p^2$, considered as the field of p^2 elements, has not a naturally-defined projective structure. If we use a generator A of the multiplicative group, then we identify the set of lines in $\mathbb{Z}_p^2$ with the set $\{1, 2, \ldots, p+1\}$: the integer $i \in \{1, 2, \ldots, p+1\}$ represents the line in $\mathbb{Z}_p^2$ spanned by A^i (see the Lemma on page 55). The resulting projective structure on the set $\{1, 2, \ldots, p+1\}$ depends on the choice of the multiplicative generator A.

We shall study examples of such structures in the next chapter.

Remark The above constructions are easily adapted to Galois fields with p^n elements (for any n).

The straight lines containing the origin form, in this case, a finite set M, the number of points of which is equal to

$$|P^m(\mathbb{Z}_p)| = \frac{p^n - 1}{p - 1} = p^m + p^{m-1} + \cdots + 1\ ,$$

where $n = m + 1$. The field table (which, remember, depends on the choice of a multiplicative generator A) defines a finite projective structure on the space $P^m(\mathbb{Z}_p)$ formed by the finite set M of these lines.

However, unlike the set-theoretical structure of M, this projective structure is *not* intrinsic: it depends on the choice of the generator A used for the identification of the field with the finite torus. Therefore, *the projective geometry of the Galois field should take into account several projective structures on the same finite set M* (whose number equals, as we shall soon see, the value of the Euler function, $\frac{1}{n}\varphi(z-1)$, for the field of $z = p^n$ elements).

The value $\varphi(x)$ of the *Euler function* is defined to be the number of those residues modulo x that are relatively prime to x. For instance, for a prime p one has $\varphi(p) = p - 1$, $\varphi(p^n) = (p-1)p^{n-1}$, and for mutually prime arguments x and y, the Euler function is multiplicative:

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) .$$

Thus,

$$\begin{array}{rr} \varphi(24) = \varphi(3)\varphi(8) = 8, & \varphi(48) = \varphi(3)\varphi(16) = 16, \\ \varphi(120) = \varphi(8)\varphi(3)\varphi(5) = 32, & \varphi(168) = \varphi(8)\varphi(3)\varphi(7) = 48. \end{array}$$

7

Projective structures: example calculations

We will now give some examples of how to calculate the projective structures of the finite projective lines generated by a field of p^2 elements and some examples of the group action of Frobenius mappings[†] on these lines and on these structures.

Consider as the simplest example the field of 25 elements; that is, the case $p = 5$. The field table was calculated on page 13 for the multiplicative generator corresponding to the matrix $(A) = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$.

The finite projective line $P^1(\mathbb{Z}_5)$ that corresponds to this field and to this table consists of $p + 1 = 6$ points, which are defined by the values of the affine coordinates $\lambda_k = u_k/v_k$ for the element A^k of the field. Thus, the table on page 13 provides the following six straight lines containing the origin:

λ	k	$k \bmod 6$
0	24, 18, 6, 12	0
1	8, 2, 14, 20	2
2	11, 5, 17, 23	5
3	10, 4, 16, 22	4
4	15, 9, 21, 3	3
∞	1, 19, 7, 13	1

The last column of this table is very useful, since it will simplify many of the calculations that follow. We shall derive it now in a more general form.

[†] We give the name Frobenius mappings (of a finite field to itself) to all the power mappings, $x \mapsto x^k$. Some of them are isomorphic mappings of the field, and they are usually called ‘Frobenius transformations’. There are more Frobenius mappings than genuine Frobenius transformations of a given Galois field.

Lemma *The straight lines containing the origin of the plane $\mathbb{Z}_p^2$ represent those sets $\{A^k\}$ of elements of the field for which $k = \text{const} \pmod{p+1}$. This congruence remains true for any choice of the multiplicative generator A defining the table $\mathbb{Z}_p^2$ of the field consisting of p^2 elements.*

Proof The condition $A^k = cA^\ell$, where c is scalar, expressing the fact that k and ℓ lie on the same line, can be written in the form

$$\text{«}A^{k-\ell} = c \text{ is a scalar element»}.$$

The *scalar subgroup* of the multiplicative group $\{A^k\}$ that has $p^2 - 1$ elements, consists of the $p - 1$ elements, $\{c = 1, c = 2, \dots, c = p - 1\}$.

The degrees s corresponding to the elements of this subgroup, $\{c = A^s\}$, form an arithmetic progression of $p - 1$ terms in the additive group $\mathbb{Z}_{z-1}$, $z = p^2$. Therefore, the step in the arithmetic progression equals $(p^2 - 1)/(p - 1) = p + 1$. Hence, this progression has the form $\{s = (p + 1)r\}$, where $r \in \{1, 2, \dots, p - 1\}$, since the element $A^{p^2-1} = 1$ belongs to the subgroup of the scalars $\{c\}$ and, hence, the point $s = p^2 - 1$ belongs to the arithmetic progression $\{s\}$.

Therefore, the necessary and sufficient condition for the non-zero elements A^k and A^ℓ of the field to belong to the same line is the relation $k - \ell = (p + 1)r$, where $r \in \mathbb{Z}_{p-1}$, thus proving the Lemma. □

Given a generator A of the multiplicative group of the field of $p^2 = 25$ elements, the set of all the multiplicative generators is formed by the powers A^s, where s is relatively prime to $p^2 - 1 = 24$. There are $\varphi(25 - 1) = 8$ of them:

$$s \in \{1, 5, 7, 11, 13, 17, 19, 23\} .$$

To see the permutation of the six points of the projective line that is produced by replacing the generator A with the generator $A_s := A^s$, we just have to take one point k for which λ attains a chosen value, and to represent A^k in terms of A_s. Since $A = A_s^r$, where $rs = 1$ in the Euler group $\Gamma(25 - 1)$, we obtain $A^k = A_s^{kr}$. Therefore, the new choice of the generator acts on each line in the same way as does the Frobenius mapping $\Phi_r = \Phi_s^{-1}$.

For this reason we shall study now the *action of the Frobenius mappings* Φ_s on our straight lines. To do so, let us calculate the affine coordinate of the image of the straight line whose affine coordinate is λ. We will denote it by

$$\lambda_s(\lambda_1) = \lambda(\Phi_s(x)) , \text{ for } \lambda(x) = \lambda_1 .$$

To calculate the function λ_s of λ_1 by these formulas, we may use the fact that the relation $x = A^k$ implies $\Phi_s(x) = A^{ks}$. Hence, to calculate $\lambda_s(\lambda_1)$, we simply have to associate to λ_1 any k provided by the preceding table, to multiply it by the number s and, then, to find the value of function λ at the product ks, which is provided by the same table (used this time in the opposite direction).

Since the value $\lambda(A^k)$ depends only on the residue of k modulo 6, it suffices to multiply by s just this residue (rather than k). This leads in few minutes to the following table for the values of all the 8 functions λ_s on all the 6 lines:

λ_1	0	1	2	3	4	∞
λ_5	0	3	∞	1	4	2
λ_7	0	1	2	3	4	∞
λ_{11}	0	3	∞	1	4	2
λ_{13}	0	1	2	3	4	∞
λ_{17}	0	3	∞	1	4	2
λ_{19}	0	1	2	3	4	∞
λ_{23}	0	3	∞	1	4	2

One can further shorten these calculations by taking into account the congruences

$$1 \equiv 7 \equiv 13 \equiv 19 \pmod{6} ,$$

which imply the congruences

$$\lambda_1 \equiv \lambda_7 \equiv \lambda_{13} \equiv \lambda_{19} ,$$

and hence the following identities for the actions $P\Phi_s$ of Φ_s on the projective line:

$$P\Phi_7 = P\Phi_{13} = P\Phi_{19} = \mathrm{Id} ;$$

here, Id is the identity transformation of $P^1(\mathbb{Z}_5)$ that leaves all of its 6 points unchanged.

Similarly, we observe the congruences

$$5 \equiv 11 \equiv 17 \equiv 23 \pmod{6} ,$$

whence

$$\lambda_5 \equiv \lambda_{11} \equiv \lambda_{17} \equiv \lambda_{23} ,$$

and therefore the corresponding Frobenius mappings act on the projective line in the same way:

$$P\Phi_5 = P\Phi_{11} = P\Phi_{17} = P\Phi_{23} .$$

Thus, we have computed the homomorphism ψ of the Euler group Γ (formed by those transformations Φ_s, or by those residues s after division by $p^2 - 1 = 24$ that are relatively prime to the number $p^2 - 1$) onto its projectivised version:

$$\psi : \{\Phi_s\} \longrightarrow \{P\Phi_s\} ,$$

where $P\Phi_s \in S(p+1)$ are the permutations of the $p+1$ straight lines containing the origin by the Frobenius mapping Φ_s of the field consisting of p^2 elements.

For the case $p = 5$ we have calculated the answers:

(1) $\Gamma \approx \mathbb{Z}_2^3$ (generated by $a = 5, b = 7, c = 13$, verifying the identities $11 = ab$, $17 = ac$, $23 = abc$);

(2) $\psi(\Gamma) \approx \mathbb{Z}_2$ (whose nontrivial element $P\Phi_5$ acts on the λ axis as the reflection of the diagram

$$\begin{array}{cccc} & & 1 & 2 \\ 0 & 4 & | & | \\ & & 3 & \infty \end{array} ;$$

in the horizontal mirror).

(3) To check whether the permutation $P\Phi_5$ of 6 points is projective, note that $0 \mapsto 0$ means that λ_5 is zero when $\lambda_1 = 0$. Therefore, if it is projective, it should have the form

$$\lambda_5 = a\lambda_1/(c\lambda_1 + d) .$$

The property $2 \mapsto \infty$ of $P\Phi_5$ implies that λ_5 should be ∞ for $\lambda_1 = 2$, and therefore one should have $2c + d = 0$. Similarly, $\infty \mapsto 2$ means that one should have $\lambda_5 = 2$ for $\lambda_1 = \infty$, and so $a = 2c$.

We obtain therefore that $d = -2c$, $a = 2c$, yielding, for the projective transformation $P\Phi_5$, the form

$$\lambda_5 = 2\lambda_1/(\lambda_1 - 2) .$$

This is indeed true for all the 6 values of λ_1.

Thus, the final conclusions are:

(1) *The projective structure on the set* $\{1, 2, 3, 4, 5, 6\}$ *does not depend on the choice of the multiplicative generator used to identify the field of order* 25 *with the finite torus*: all the 8 choices lead to the same projective structure.

(2) *The kernel of the projectivisation homomorphism* ψ *consists of the four Frobenius mappings that leave unchanged every straight line containing* 0: $\{\Phi_1, \Phi_7, \Phi_{13}, \Phi_{19}\}$. This kernel forms a group isomorphic to $\mathbb{Z}_2^2$.

(3) *The image of the projectivisation homomorphism ψ is isomorphic to $\mathbb{Z}_2$.* Its only nontrivial permutation of the 6 points of the finite projective line $P^1(\mathbb{Z}_5)$ leaves unchanged the points $\lambda_1 = 0$ and $\lambda_1 = 4$ and permutes $\lambda_1 = 1$ with $\lambda_1 = 3$ and $\lambda_1 = 2$ with $\lambda_1 = \infty$.

This projective transformation is defined by the formula

$$\lambda_5 = \frac{2\lambda_1}{\lambda_1 - 2}$$

and is generated by the automorphism Φ_5 of the field of 25 elements. This automorphism satisfies the identity

$$\Phi_5(x + y) = \Phi_5(x) + \Phi_5(y) ,$$

which is not satisfied by Φ_7.

The calculations of the projective structures and of the Frobenius mappings (which may or may not be Frobenius automorphisms) for fields consisting of p^2 elements with other prime numbers p follows the same lines as in the case $p = 5$ studied above. But the resulting answers are so different for the different primes ($p = 7, 11, 13$), that I cannot even begin to guess some general conclusions for higher values of p.

The case $p = 7$

The Euler group $\Gamma(48)$ consists of

$$\varphi(p^2 - 1) = \varphi(48) = \varphi(3)\,\varphi(16) = 16 \text{ residues modulo } 48$$

relatively prime to 48:

$$\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\} .$$

This multiplicative group is isomorphic to the direct product $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with generators 5 for the factor $\mathbb{Z}_4$ and 7, 17 for the factors $\mathbb{Z}_2$.

The 8 points of the finite projective line $P^1(\mathbb{Z}_7)$ that correspond to the elements A^k of the field, where $(A) = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$, are defined by the corresponding residues of the exponents k modulo $p + 1 = 8$, as follows:

$\lambda_1(A^k)$	0	1	2	3	4	5	6	∞
k (mod 8)	0	2	6	7	5	3	4	1

(see the field table on page 15).

The actions of the generators of the Euler group represented by the Frobenius mappings Φ_5, Φ_7 and Φ_{17}, provide the following values of the functions λ_5, λ_7, λ_{17} (calculated, multiplying k by s, using the algorithm described in detail earlier for the case $p = 5$): $\lambda_k(\lambda) = \lambda_1(\Phi_k(x))$, for $\lambda_1(x) = \lambda$:

λ_1	0	1	2	3	4	5	6	∞
λ_5	0	1	2	5	∞	3	6	4
λ_7	0	2	1	∞	5	4	6	3
λ_{17}	0	1	2	3	4	5	6	∞

We need no new calculations for $P\Phi_{17}$, since $17 \equiv 1 \pmod 8$; therefore, the permutation $P\Phi_{17} = P\Phi_1 = \mathrm{Id}$ is the identity transformation of the finite projective line $P^1(\mathbb{Z}_7)$ (i.e. it leaves each point of this line unchanged: $\lambda_{17} \equiv \lambda_1$).

The permutations $P\Phi_5$ and $P\Phi_7$ act on the points corresponding to the different values of λ as symmetries (with respect to a horizontal mirror) of the following two diagrams, whose points represent the points of P^1 denoted by their coordinate λ_1:

The case $P\Phi_5$

$$\begin{array}{cccccc} 3 & 4 & & & & \\ | & | & 0 & 1 & 2 & 6\,; \\ 5 & \infty & & & & \end{array}$$

The case $P\Phi_7$

$$\begin{array}{ccccc} 1 & 3 & 4 & & \\ | & | & | & 0 & 6\,. \\ 2 & \infty & 5 & & \end{array}$$

The first permutation ($P\Phi_5$) is not projective, since it has four fixed points (such a projective mapping ought to be the identity, leaving unchanged all the 8 points).

For the second permutation ($P\Phi_7$) we deduce the following: from $0 \mapsto 0$, we deduce that $\lambda_7 = \frac{a\lambda_1}{c\lambda_1+d}$; from $3 \mapsto \infty$, it follows that $3c + d = 0$; while $\infty \mapsto 3$ implies the relation $a = 3c$. Thus, in the case that the permutation $P\Phi_7$ is projective, the values of λ_7 ought everywhere to be equal to $3\lambda_1/(\lambda_1 - 3)$, and this is indeed the case in the above table. Thus, the permutation $P\Phi_7$ is projective (i.e. preserves the projective structure).

Multiplying the permutations that we have already calculated, we obtain the complete projectivisation homomorphism $\psi : (\Gamma \approx \{\Phi_s\}) \to \{P\Phi_s\}$.

The resulting conclusions are:

(1) *The field consisting of* 49 *elements generates two different projective structures on the set* $\mathbb{Z}_8 = \{0, 1, \ldots, 7\}$*, depending on the choice of the multiplicative generator used to identify* $P^1(\mathbb{Z}_7)$ *with this set. The permutation* $P\Phi_5$ *sends one of these two structures to the other.*

The difference between these structures is analogous to the difference between old and new railway schedules when the only change is that some cities have been renamed.

(2) *The permutation* $P\Phi_7$ *preserves both projective structures of the set of* 8 *elements:* $\{k \pmod 8\}$.

(3) *The permutation* $P\Phi_{17} = P\Phi_1$ *is the identity, leaving unchanged every point of the set* $P^1(\mathbb{Z}_7)$. The Frobenius mapping Φ_{17} belongs to the kernel of the projectivisation homomorphism ψ. This kernel consists of the four Frobenius mappings Φ_s:

$$\operatorname{Ker} \psi = \{\Phi_1, \Phi_{17}, \Phi_{25}, \Phi_{41}\} ,$$

for which s is congruent to 1 modulo 8. This group is isomorphic to the group $\mathbb{Z}_2^2$ (for example, $\Phi_{17}\Phi_{25} = \Phi_{41}$).

(4) *The image of the projectivisation homomorphism* ψ *is also isomorphic to the group* $\mathbb{Z}_2^2$. It consists of the four permutations $\{P\Phi_1, P\Phi_5, P\Phi_7, P\Phi_{11}\}$, of which $P\Phi_1 = \mathrm{Id}$ and $P\Phi_7$ are biprojective (preserving both projective structures), while each permutation $P\Phi_5$ and $P\Phi_{11}$ permutes the two projective structures of the set $P^1(\mathbb{Z}_7)$.

The Frobenius mapping Φ_7 is an automorphism of the field consisting of 49 elements, $\Phi_7(x + y) = \Phi_7(x) + \Phi_7(y)$; this does not hold for Φ_5 or for Φ_{11}.

Thus, the group $\{P\Phi_s\} \approx \mathbb{Z}_2^2$ acts on the two projective structures of the set $P^1(\mathbb{Z}_7)$, as $\mathbb{Z}_2$ (with kernel $\{P\Phi_1, P\Phi_7\}$ generated by the Frobenius automorphisms of the field).

To obtain the first or the second projective structure defined by the coordinates k mod 8 of the function $\lambda = \lambda_k$ of the set of eight elements $\mathbb{Z}_8$, one has to choose the following generators, A^s, of the multiplicative group (as is implied by the field table on page 15):

P_1	1, 7, 17, 23	25, 31, 41, 47	$s = 8r \pm 1$
P_5	5, 11, 13, 19	29, 35, 37, 43	$s = 8r \pm 3$

The Frobenius mappings of the first line (where $s = 8r \pm 1$) *preserve both the projective structures* P_1 *and* P_5*, while those of the second* (where $s = 8r \pm 3$) *permute the projective structures* P_1 *and* P_5 *on the set* $\mathbb{Z}_8$.

The case $p = 11$

The Euler group $\Gamma(120)$ consists of $\varphi(p^2 - 1) = \varphi(120) = \varphi(3)\,\varphi(5)\,\varphi(8) = 32$ residues modulo 120, relatively prime to 120: they are the residues

$$\{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, \dots\}\,,$$

including $120 - s$ together with s.

This multiplicative group is isomorphic to the direct product $\mathbb{Z}_4 \times \mathbb{Z}_2^3$ (with generators 7 for $\mathbb{Z}_4$ and $11, 19, 61$ for the three factors $\mathbb{Z}_2$).

Since the matrix (A) is $\begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix}$, the 12 points of the projective line $P^1(\mathbb{Z}_{11})$ corresponding to the elements A^k of the field depend in the following way on the residues modulo $p + 1 = 12$ of the numbers k:

$\lambda_1(A^k)$	0	1	2	3	4	5	6	7	8	9	10	∞
k (mod 12)	0	9	7	5	2	3	8	4	10	6	11	1

This follows from the field table on page 15.

The action of the generators of the Euler group by the Frobenius mappings Φ_7, Φ_{11}, Φ_{19} and Φ_{61} (which determine the respective permutations $P\Phi_7, \dots, P\Phi_{61}$ of the 12 points forming $P^1(\mathbb{Z}_{11})$) provides the following table for the values of the functions λ_7, λ_{11}, λ_{19} and λ_{61} on the coordinates k (mod 12) of the points of the set P^1:

$$\lambda_s(\lambda_1(x)) := \lambda_1(\Phi_s(x))\,.$$

As explained previously (for $p = 5$), the calculation of $\lambda_s(\lambda_1)$ from the table on page 61 follows the algorithm

$$(\lambda_1 \mapsto k)\,,\ (k \mapsto sk)\,,\ (sk \mapsto \lambda_1(A^{sk}))\,,$$

where we first use this table the downstairs ($\downarrow$) way and at the end, the opposite, upstairs way ($\uparrow$).

These calculations have to be performed only for one representative of each of the four modulo 12 classes of the numbers $s \in \Gamma$:

Γ_1	$1 \sim 13 \sim 37 \sim 49 \sim 61 \sim 73 \sim 97 \sim 109$
Γ_7	$7 \sim 19 \sim 31 \sim 43 \sim 67 \sim 79 \sim 91 \sim 103$
Γ_{11}	$11 \sim 23 \sim 47 \sim 59 \sim 71 \sim 83 \sim 107 \sim 119$
Γ_{17}	$17 \sim 29 \sim 41 \sim 53 \sim 77 \sim 89 \sim 101 \sim 113$

In the case where s belongs to Γ_1, the mapping $P\Phi_s$ is the identity; hence, $\lambda_1 = \lambda_{13} = \lambda_{37} = \cdots = \lambda_{109}$.

To calculate the permutation $P\Phi_{17}$ and the functions $\lambda_{17} = \lambda_{29} = \cdots = \lambda_{113}$, it suffices to multiply the permutations $P\Phi_7$ and $P\Phi_{11}$ (since $7 \cdot 11 = 77 \in \Gamma_{17}$). It remains, therefore, to calculate the functions λ_7 and λ_{11}, for which the values are provided by the values of $\lambda_1(A^k)$ in the table on page 61 (using the algorithm $\lambda_1 \mapsto k \mapsto sk \mapsto \lambda_1(A^{sk})$):

λ_1	0	1	2	3	4	5	6	7	8	9	10	∞
λ_7	0	5	∞	10	4	1	6	7	8	9	3	2
λ_{11}	0	5	3	2	8	1	7	6	4	9	∞	10
λ_{17}	0	1	10	∞	8	5	7	6	4	9	2	3

The permutations $P\Phi_7$, $P\Phi_{11}$ and $P\Phi_{17}$ permute the 12 points of the finite projective line $P^1(\mathbb{Z}_{11})$. Denoting the points of this set by the values of the coordinate λ_1, we can describe these permutations as the (horizontal) mirror symmetries of the following three diagrams:

The case $P\Phi_7$

$$\begin{array}{ccccccccc} 1 & 2 & 3 & & & & & & \\ | & | & | & 0 & 4 & 6 & 7 & 8 & 9\,, \\ 5 & \infty & 10 & & & & & & \end{array}$$

The case $P\Phi_{11}$

$$\begin{array}{ccccccc} 1 & 2 & 4 & 6 & 10 & & \\ | & | & | & | & | & 0 & 9\,, \\ 5 & 3 & 8 & 7 & \infty & & \end{array}$$

The case $P\Phi_{17}$

$$\begin{array}{cccccccc} 2 & 3 & 4 & 6 & & & & \\ | & | & | & | & 0 & 1 & 5 & 9\,. \\ 10 & \infty & 8 & 7 & & & & \end{array}$$

These diagrams imply that the involutions $P\Phi_7$ and $P\Phi_{17}$ do not preserve the projective structure P_1 of the finite line $P^1(\mathbb{Z}_{11})$ (which is defined by the coordinate λ_1), while the involution $P\Phi_{11}$ does preserve it, since $\lambda_{11} = -\frac{\lambda_1}{\lambda_1+1}$ is a fractional-linear function.

Both the permutations $P\Phi_7$ and $P\Phi_{17}$ send the projective structure P_1 to the same image projective structure:

$$P_7 := (P\Phi_7)(P_1) = P_{17} := (P\Phi_{17}(P_1))\,,$$

where the functions λ_7 and λ_{17} are fractional-linearly related:

$$\lambda_{17} = -\frac{\lambda_7}{\lambda_7 + 1} .$$

The permutation $P\Phi_{11}$ (generated by the Frobenius automorphism Φ_{11} of the field consisting of 121 elements) preserves both the projective structures, P_1 and ($P_7 = P_{17}$), on the set $\mathbb{Z}_{12}$ consisting of 12 points, while each of the two permutations $P\Phi_7$ and $P\Phi_{17}$ permutes these two structures, P_1 and P_7.

The kernel of the projectivisation homomorphism

$$\psi : (\Gamma \approx \{\Phi_s\}) \to \{P\Phi_s\},$$

consists of the eight Frobenius mappings Φ_s forming Γ_1, where $s = 12r + 1$; that is, where $s \in \{1, 13, 37, 49, 61, 73, 97, 109\}$. These eight mappings form the group $\operatorname{Ker}\psi \approx \mathbb{Z}_4 \times \mathbb{Z}_2$ (whose generators correspond to $s = 13$ for $\mathbb{Z}_4$ and to $s = 61$ for $\mathbb{Z}_2$).

The image of the projectivisation homomorphism ψ consists of the four permutations $\{P\Phi_1, P\Phi_7, P\Phi_{11}, P\Phi_{17}\}$, which form a group isomorphic to $\mathbb{Z}_2^2$. Its action on the set of points of the projective line $P^1(\mathbb{Z}_{11})$ and on its two projective structures P_1 and P_7 (provided by the coordinate functions $\lambda = \lambda(k)$ defined by the field of 121 elements for different choices of the generator of the multiplicative group) is described above: in particular, $P\Phi_{17} = (P\Phi_{11})(P\Phi_7)$, $(P\Phi_{11})(P\Phi_{11}) = (P\Phi_7)(P\Phi_7) = 1$.

All these facts mean that the Euler group, which is represented by 32 Frobenius mappings, acts on the set of the two projective structures P_1 and P_7 on the coordinates k (mod 12) of the points of the finite projective line (generated by the field of 121 elements) as the group $\mathbb{Z}_2$ of the permutations of these two structures. Both structures remain fixed under the 16 mappings $P\Phi_s$ for which $s = 12r \pm 1$ ($r \in \mathbb{Z}$): that is, for s belonging to the above lists Γ_1 and Γ_{11}. The 16 permutations $P\Phi_s$, for which $s = 12r \pm 5$ ($r \in \mathbb{Z}$) (i.e. those for which s belongs to the above lists Γ_7 and Γ_{17}) send P_1 to P_7 and P_7 to P_1.

Thus, the kernel of the homomorphism $\psi : \Gamma \to \mathbb{Z}_2$, defined by the actions of the Frobenius mappings on the projective structures, is

$$\operatorname{Ker}\psi = \Gamma_1 \cup \Gamma_{11} \approx \mathbb{Z}_4 \times \mathbb{Z}_2^2 ,$$

with generators corresponding to Φ_{13} for the factor $\mathbb{Z}_4$ and to Φ_{61} and Φ_{11} for the factors $\mathbb{Z}_2$.

Case $p = 13$

The Euler group $\Gamma(168)$ consists of the

$$\varphi(p^2 - 1) = \varphi(168) = \varphi(3) \cdot \varphi(7) \cdot \varphi(8) = 48$$

residues modulo 168, relatively prime to 168. Namely,

$$\Gamma(168) = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47,\\ 53, 55, 59, 61, 65, 67, 71, 73, 79, 83, 85, \dots\} ,$$

where the residue $168 - s$ is included together with the residue s.

This group is isomorphic to the product of four cyclic groups: $\Gamma(168) \simeq \mathbb{Z}_6 \times \mathbb{Z}_2^3$, with generators 5 for $\mathbb{Z}_6$, 29, 43 and 85 for the second-order factors.

The 14 points of the projective line $P^1(\mathbb{Z}_{13})$ that correspond to elements A^k of the field for the chosen generator $(A) = \begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix}$, are defined by the residues of k modulo $p + 1 = 14$, in the following way:

$\lambda_1(A^k)$	0	1	2	3	4	5	6	7	8	9	10	11	12	∞
k (mod 14)	0	8	2	13	11	6	7	12	4	9	10	5	3	1

(this is implied, in fact, by the table on page 16).

The actions of the generators of the Euler group by the Frobenius mappings $\{\Phi_5, \Phi_{29}, \Phi_{43}, \Phi_{85}\}$ give the values of the functions λ_5, λ_{29}, λ_{43} and λ_{85} via the usual algorithm:

$$(\lambda_1 \mapsto k) , \ (k \mapsto sk) , \ (\lambda_s = \lambda_1(A^{sk})) .$$

It follows that the resulting permutation $P\Phi_s$ depends only on the residue of s modulo $p + 1 = 14$ and, therefore, the Euler group $\Gamma(168)$ is subdivided into six classes of residues s (mod 168), equiresidual modulo 14:

$$\Gamma_1 = \{1, 29, 43, 71, 85, 113, 127, 155\} , \quad s = 14r + 1 ;$$

$$\Gamma_5 = \{5, 19, 47, 61, 89, 103, 131, 145\} , \quad s = 14r + 5 ;$$

$$\Gamma_{11} = \{11, 25, 53, 67, 95, 109, 137, 151\} , \quad s = 14r - 3 ;$$

$$\Gamma_{13} = \{13, 41, 55, 83, 97, 125, 139, 167\} , \quad s = 14r - 1 ;$$

$$\Gamma_{17} = \{17, 31, 59, 73, 101, 115, 143, 157\} , \quad s = 14r + 3 ;$$

$$\Gamma_{23} = \{23, 37, 65, 79, 107, 121, 149, 163\} , \quad s = 14r - 5 ;$$

The table on page 64, which relates k to $\lambda_1(A^k)$, gives the following values for the functions λ_s:

λ_1	0	1	2	3	4	5	6	7	8	9	10	11	12	∞
λ_5	0	7	10	9	3	2	6	8	5	12	1	4	∞	11
λ_{11}	0	8	1	12	9	10	6	5	2	∞	7	3	11	4
λ_{13}	0	5	7	∞	12	1	6	2	10	11	8	9	4	3
λ_{17}	0	10	5	4	11	8	6	1	7	3	2	∞	9	12
λ_{23}	0	2	8	11	∞	7	6	10	1	4	5	12	3	9

Therefore, the permutation $P\Phi_5$ acts on the 14 points of the set $P^1(\mathbb{Z}_{13})$ in the following strange way:

$$\begin{tikzcd}
P\Phi_5 : & 1 \arrow[r, mapsto] & 7 \arrow[r, mapsto] & 8 \arrow[d, mapsto] & 3 \arrow[r, mapsto] & 9 \arrow[r, mapsto] & 12 \arrow[d, mapsto] & 0 \arrow[loop right] & 6 \arrow[loop right] \\
 & 10 \arrow[u, mapsto] & 2 \arrow[l, mapsto] & 5 \arrow[l, mapsto] & 4 \arrow[u, mapsto] & 11 \arrow[l, mapsto] & \infty \arrow[l, mapsto] & &
\end{tikzcd}$$

We have denoted here the points of the finite projective line by their affine coordinates $\lambda_1(A^k)$. We see that the permutation $P\Phi_5$ has two long orbits each consisting of six points, and has two fixed points. It is useful to observe that $(P\Phi_5)^6 = 1$.

The permutation $P\Phi_5$ is not a projective transformation. For otherwise we would have

$$\lambda_5 = \frac{a\lambda_1}{c\lambda_1 + d}\,,$$

since $\lambda_5 = 0$ for $\lambda_1 = 0$. Therefore, the condition $\lambda_5 = \infty$ for $\lambda_1 = 12$ would mean that $12c + d = 0$, while the condition $\lambda_5 = 11$ for $\lambda_1 = \infty$ would mean $a = 11c$. Thus, the projective permutation $P\Phi_5$ would be $\lambda_5 = 11\lambda_1/(\lambda_1 - 12)$, and this would yield, for $\lambda_1 = 1$, the value $\lambda_5 = 11/(-11) = 12$, contradicting the above table, which claims $\lambda_5(\lambda_1 = 1) = 7$.

This contradiction shows that the permutation $P\Phi_5$ does not preserve the usual projective structure P_1, but sends it to the projective structure P_5, which is represented by the affine coordinate λ_5 on $\{k \pmod{14}\}$.

The permutation $P\Phi_{11}$ permutes the 14 points of the set $P^1(\mathbb{Z}_{13})$, denoted by their coordinates λ_1, in the following strange way:

$$\begin{tikzcd}
P\Phi_{11} \quad : & & & & & & & & \\
1 \arrow[rr, mapsto] & & 8 \arrow[dl, mapsto] & 3 \arrow[rr, mapsto] & & 12 \arrow[dl, mapsto] & 4 \arrow[rr, mapsto] & & 9 \arrow[dl, mapsto] \\
& 2 \arrow[ul, mapsto] & & & 11 \arrow[ul, mapsto] & & & \infty \arrow[ul, mapsto] & \\
5 \arrow[rr, mapsto] & & 10 \arrow[dl, mapsto] & 0 \arrow[loop right, mapsto] & 6 \arrow[loop right, mapsto] & ; & & & \\
& 7 \arrow[ul, mapsto] & & & & & & &
\end{tikzcd}$$

two fixed points and four orbits, each consisting of 3 points. Note that $P\Phi_{11} = (P\Phi_5)^2$ and that $(P\Phi_{11})^3 = 1$.

If the permutation $P\Phi_{11}$ were projective, it would have the form $\lambda_{11} = a\lambda_1/(c\lambda_1 + d)$, since $0 \mapsto 0$, and the action $9 \mapsto \infty$ would imply $9c + d = 0$, while the action $\infty \mapsto 4$ would imply $a = 4c$. Thus, $P\Phi_{11}$ would have the form

$$\lambda_{11} = \frac{4\lambda_1}{\lambda_1 - 9} \, .$$

Therefore, we would obtain the value

$$\lambda_{11}(\lambda_1 = 1) = 4/(-8) = -20 = 6 \ (\mathrm{mod}\ 13) \, ,$$

contradicting the value $\lambda_{11}(\lambda_1 = 1) = 8$ in the table on page 65.

Therefore the non-projective permutation $P\Phi_{11}$ sends the standard projective structure P_1 associated to the affine coordinate λ_1 to the projective structure P_{11} of the same set $\{k \ (\mathrm{mod}\ 14)\}$, associated to the affine coordinate λ_{11}.

The permutation $P\Phi_{13}$ is a projective transformation, since it is generated by the Frobenius automorphism Φ_{13} of the field of 169 elements.

Its projectivity is also evident from the values of the function λ_{13} in the table on page 65: denoting the points of P^1 by their coordinate λ_1, we get the permutation action.

The case $P\Phi_{13}$

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 8 & 9 & & \\ | & | & | & | & | & | & 0 & 6\,; \\ 5 & 7 & \infty & 12 & 10 & 11 & & \end{array}$$

this diagram implies that $\lambda_{13} = -\lambda_1/(4\lambda_1 + 1)$.

The remaining permutations $P\Phi_s$, for $s = 17$ and 23, can now be obtained by simple multiplications: we note that

$$13 \cdot 5 = 65 \in \Gamma_{23}\ , \quad 13 \cdot 11 = 143 \in \Gamma_{17}$$

and, therefore, we have the following identities for the permutation products:

$$P\Phi_{23} = (P\Phi_5)(P\Phi_{13})\ , \quad P\Phi_{17} = (P\Phi_{11})(P\Phi_{13})\ .$$

Thus, the permutation $P\Phi_{23}$ sends the structure P_1 to the structure P_5 (the first permutation $P\Phi_{13}$ sends the structure P_1 to itself, and the next permutation $P\Phi_5$ transforms P_1 into P_5).

Similarly the permutation $P\Phi_{17}$ sends the structure P_1 to P_{11}.

Since the permutation $P\Phi_{13}$ preserves P_5, it also preserves each of the structures P_5 and P_{11}. Hence, the permutation $P\Phi_{23}$ preserves the structure P_1 and the permutation $P\Phi_{17}$ preserves the structure P_{11}.

To study the action of the permutation $P\Phi_5$ on the structure P_{11}, it suffices to use the affine coordinate λ_{11}, counting the value of λ_{11} at the point x^5, given the value $\lambda_{11}(x)$. Since the product $(P\Phi_{11})(P\Phi_5)$ of the permutations is $P\Phi_{13}$ (because $55 \in \Gamma_{13}$), we get

$$\lambda_{11}(x^5) := \lambda_1(x^{55}) = \lambda_1(x^{13}) := \lambda_{13}(x)\ ,$$

and, therefore, we should be able to calculate the dependence of $\lambda_{13}(x)$ on $\lambda_{11}(x)$. Our table of the values of the functions λ_s (see page 65) provides this dependence:

$\lambda_{11}(x)$	0	1	2	3	4	5	6	7	8	9	10	11	12	∞
$\lambda_{13}(x)$	0	7	10	9	3	2	6	8	5	12	1	4	∞	11

Therefore, the transformation $P\Phi_5$ acts on the expression for the coordinates of the structure P_{11} in the same way as it acts on the formula for the structure P_1: the structure P_{11} is sent to the projective structure P_{13}, which is defined by the affine coordinate λ_{13}.

But the structure P_{13} coincides with P_1, since the Frobenius mapping Φ_{13} is an automorphism of the field of 169 elements. Therefore, *the action of the transformation* Φ_5 *on the three projective structures (generated by the field of* 169 *elements) is given by the triangular diagram*

$$\begin{tikzcd}
P\Phi_5 \quad : & P_1 \arrow[rr, mapsto] & & P_5 \; ; \arrow[dl, mapsto] \\
& & P_{11} \arrow[ul, mapsto] &
\end{tikzcd}$$

it sends the structure P_5 to the structure P_{11}, since $5 \cdot 5 = 25 \in \Gamma_{11}$.

Similarly, one may calculate the action of the permutation $P\Phi_{11}$ on these three structures. But one can avoid new calculations, since

$$P\Phi_{11} = (P\Phi_5)^2$$

and, therefore, it acts as the cyclic transformation of order 3, inverse to the action of $P\Phi_5$. We get the triangular diagram of the action of $P\Phi_{11}$ on the three projective structures,

$$\begin{tikzcd}
P\Phi_{11} \quad : & P_1 \arrow[rr, mapsto] & & P_{11} \; . \arrow[dl, mapsto] \\
& & P_5 \arrow[ul, mapsto] &
\end{tikzcd}$$

The description of the kernel and of the image of projectivisation homomorphism

$$\psi : (\Gamma \approx \{\Phi_s\}) \longrightarrow \{P\Phi_s\} ,$$

is also implicitly contained in our explicit formulas for the permutations $P\Phi_s$.

The answers are the three isomorphisms

$$\Gamma \approx (\mathbb{Z}_6 \times \mathbb{Z}_2^3) , \quad \text{Ker}\, \psi \approx \mathbb{Z}_2^3 , \quad \text{Im}\, \psi \approx \mathbb{Z}_6 .$$

Namely, *the kernel consists of eight Frobenius mappings* Φ_s*, where* s *belongs to the class* Γ_1 (for which $s = 14r + 1$).

One may, for instance, take as the generators of the kernel the transformations Φ_{29}, Φ_{43}, Φ_{85}, taking into account the following relations for the Frobenius mappings:

$$\Phi_{71} = \Phi_{29}(\Phi_{43}) , \quad \Phi_{113} = \Phi_{29}(\Phi_{85}) , \quad \Phi_{127} = \Phi_{43}(\Phi_{85}) ,$$
$$\Phi_{155} = \Phi_{29}(\Phi_{43}(\Phi_{85})) .$$

One can take the 6th-order permutation $g = P\Phi_5$ as the generator of the image group. The image consists of its powers, i.e. the following identities hold:

$$g^2 = P\Phi_{11}\ ,\ g^3 = P\Phi_{13}\ ,\ g^4 = P\Phi_{37}\ ,\ g^5 = P\Phi_{17}\ ,\ g^6 = 1,$$

since $5^2 \in \Gamma_{11}, 5^3 \in \Gamma_{13}, 5^4 \in \Gamma_{37}, 5^5 \in \Gamma_{17}$.

The permutation g acts cyclically on the three projective structures P_1, P_5, P_{11} (generated by the field consisting of 169 elements). The permutation g^3 leaves each of these three structures unchanged, since it is generated by the Frobenius automorphism of the field. We have thus described the entire situation for $p = 13$.

Unfortunately, I have neither theorems, nor even conjectures, to extend the above description of projective geometry to fields with more elements, not even in the case of p^2 elements with higher primes p, where the geometry remains 1-dimensional.

To find these generalisations one will probably have first to calculate the formulas $\lambda = \lambda(k)$ that describe the projective structures in terms of the projective line coordinate k (mod $p + 1$) and the action of the Frobenius mappings on these structures (at least for the case of the field of p^2 elements) so that we get more examples. The fact that the answers in the cases $p = 5, 7, 11$ and 13 discussed above are so heterogeneous obstructs attempts to guess the general rules for higher values of p.[†] The number $|P^1(\mathbb{Z}_n)|$ of points of the projectivised version of the affine line $\mathbb{Z}_n$ equals $nK(n)$, where $K(n) = \prod(1 + 1/p)$ over the prime divisors p of n (being thus $1 + 1/p$ for prime numbers $n = p$). For some special integers, starting with $K(6) = 2$, the quantity K attains arbitrary large values. However, according to F. Aicardi, the Cesaro average $\hat{K}(n) = (K(1) + \cdots + K(n))/n$ of the coefficients $K(n)$ tends, as $n \to \infty$, to a constant, namely, to $\hat{K}_\infty(n) = \frac{15}{\pi^2} = \frac{\zeta(2)}{\zeta(4)}$.

[†] In fact, for prime p, one can indeed prove that the number of different projective structures on a set of $p + 1$ elements that is generated by a Galois field of p^2 elements is given by $\frac{1}{2}\varphi(p + 1)$.

8

Cubic field tables

To help the reader to conduct further experimental studies, I provide in this chapter the tables of the fields of 8, 27, 125, 16 and 81 elements. In the case of p^3 elements I shall use the additive basis $\{1, A, A^2\}$, choosing first some generator A of the multiplicative group.

The table fills the cells (u, v, w) of a finite cube (torus) $\mathbb{Z}_p^3$ by the degrees k of the powers A^k of the multiplicative generator:

$$A^k = u_k A^2 + v_k A + w_k 1 \ .$$

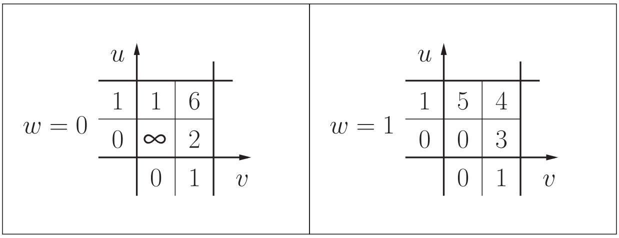
To show how this cube is filled, I shall present below its plane square sections $w =$ const. filled with the degrees k.

The presence of the number k (mod $p^2 - 1$) in the cell (u, v) of the square w in the table means we have the identity

$$A^k = uA^2 + vA + w1 \ .$$

The tables are shown below for the square sections of the cube (torus) for $p = 2$, 3 and 5.

Table of the field consisting of 2^3 elements



$w = 0$

u		
1	1	6
0	∞	2
	0	1
		v

$w = 1$

u		
1	5	4
0	0	3
	0	1
		v

The table corresponds to the matrix

$$(A) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} .$$

The six elements A^k for which $1 \leq k \leq 6$ are primitive (generators). The table implies the four identities $A^3 = A^2 + 1$, $A^4 = A^2 + A + 1$, $A^5 = A^2 + 1$, $A^6 = A^2 + A$. These identities follow recursively from the first one.

Table of the field consisting of 3^3 elements

v				
2	14	12	6	
1	**1**	**19**	**25**	
0	∞	2	**15**	
	0	1	2	u

w= 0

v				
2	24	20	**21**	
1	18	22	**17**	
0	0	**7**	16	
	0	1	2	u

w= 1

v				
2	**5**	**9**	4	
1	**11**	8	**23**	
0	13	**3**	20	
	0	1	2	u

w= 2

The multiplicative generator that was used here corresponds to the matrix

$$(A) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 1 \end{pmatrix} .$$

The table yields $3^3 - 2 = 25$ identities, including, for example,

$$A^0 = 1 \ , \ A^3 = A^2 + 2 \ , \ A^4 = A^2 + 2A + 2 \ ,$$

$$A^5 = 2A + 2 \ , \ A^6 = 2A^2 + 2A \ , \ A^7 = A^2 + 1 \ ,$$

$$A^8 = A^2 + A + 2 \ , \ A^9 = 2A^2 + 2A + 2 \ , \ \dots \ ,$$

$$A^{24} = 2A + 1 \ , \ A^{25} = 2A^2 + A \ , \ A^{26} = 1 \ .$$

All these identities follow recursively from the second one of this list, which means that matrix (A) satisfies its own characteristic equation.

The number of generators A^k of the multiplicative group (where $1 \leq k \leq 25$) equals $\varphi(3^3 - 1) = 12$. These 12 values of the degree k are represented in the table as bold characters.

Table of the field consisting of 5^3 elements

u						
4	**63**	**85**	**69**	112	92	
3	32	**81**	54	**61**	38	
2	94	100	**123**	116	**19**	
1	**1**	30	50	**7**	**23**	
0	∞	2	**95**	**33**	34	
	0	1	2	3	4	v

$w = 0$

u						
4	22	88	10	**35**	98	
3	6	44	78	**83**	46	
2	**49**	58	28	**25**	14	
1	**29**	**79**	**11**	**71**	12	
0	124	**55**	70	96	**51**	
	0	1	2	3	4	v

$w = 1$

u						
4	18	118	**27**	**107**	**121**	
3	**115**	4	**57**	**67**	**103**	
2	122	40	48	**105**	104	
1	**99**	52	**13**	**15**	**47**	
0	93	**65**	24	20	**39**	
	0	1	2	3	4	v

$w = 2$

u						
4	**37**	**109**	**77**	**75**	114	
3	60	42	**43**	110	102	
2	**53**	**41**	**5**	**119**	66	
1	80	**59**	**45**	**89**	56	
0	31	**101**	82	86	**3**	
	0	1	2	3	4	v

$w = 3$

u						
4	**91**	74	**9**	**73**	**17**	
3	**111**	76	**87**	90	120	
2	68	108	**21**	16	106	
1	84	36	**97**	72	26	
0	62	**113**	34	8	**117**	
	0	1	2	3	4	v

$w = 4$

$$(A) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 4 \end{pmatrix}$$

This table announces $5^3 - 2 = 123$ congruences:

$$A^0 = 1\ ,\ \ A^3 = 4A^2 + 3\ ,\ \ A^4 = A^2 + 3A + 2\ ,$$

$$A^5 = 2A^2 + 2A + 3\ ,\ \ A^6 = 3A + 1\ , \ldots$$

$$\ldots,\ A^{63} = 4A\ ,\ \ldots\ ,\ A^{114} = 4A^2 + 4A + 3\ ,\ldots$$

$$A^{123} = 2A^2 + 2A\ ,\ A^{124} = 1\ .$$

All these identities follow recursively from the second one, which means the matrix (A) satisfies its characteristic equation.

The number of generators A^k of the multiplicative group (where $1 \le k \le 123$) equals $\varphi(5^3 - 1) = \varphi(31)\ \varphi(4) = 60$. These 60 values of k are shown in the above field table as bold characters.

For fields consisting of p^4 elements, we choose the additive generators $1, A, A^2, A^3$, where A is a generator of the multiplicative group.

The field table fills (by the exponents k of the elements A^k) the cells (u, v, w, t) of the finite four-dimensional cube (torus) $\mathbb{Z}_p^4$:

$$A^k = u_k A^3 + v_k A^2 + w_k A + t_k 1\ .$$

To show this, we present below its two-dimensional plane sections ($w =$ const, $t =$ const).

The appearance of the number k (where $1 \le k \le p^4 - 2$) in the cell (u, v) of the square numbered (w, t) gives the identity

$$A^k = uA^3 + vA^2 + wA + t1\ .$$

These squares form the following tables, calculated for $p = 2$ and for $p = 3$.

Table of the field consisting of 2^4 elements

u		
1	9	**11**
0	0	**1**
	0	1	v

$w = 0,\ t = 1$

u		
1	**7**	6
0	12	5
	0	1	v

$w = t = 1$

u		
1	**2**	**14**
0	∞	3
	0	1	v

$w = t = 0$

u		
1	**13**	**8**
0	**1**	10
	0	1	v

$w = 1,\ t = 0$

This table was computed for the generator of the multiplicative group that is defined in the matrix representation of the field by the matrix

$$(A) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} .$$

The table above is the geometric shorthand description of the $2^4 - 3 = 13$ identities:

$$A^0 = 1 \, , \; A^4 = A^3 + 1 \, , \; A^5 = A^3 + A + 1 \, ,$$

$$A^6 = A^3 + A^2 + A + 1 \, , \dots \, , \; A^{14} = A^3 + A^2 \, , \; A^{15} = 1 \, .$$

These identities follow recursively from the second one, which means the matrix (A) satisfies its characteristic equation.

The number of generators A^k of the multiplicative group (where $1 \leq k \leq 14$) equals $\varphi(2^4 - 1) = \varphi(3)\,\varphi(5) = 8$. These eight values of the exponent k are shown in the table as bold characters.

Table of the field consisting of 3^4 elements

v				
2	18	20	36	
1	65	**27**	50	
0	40	44	**31**	
	0	1	2	u

$w = 0, t = 2$

v				
2	34	46	**7**	
1	**23**	**73**	**13**	
0	68	5	**61**	
	0	1	2	u

$w = 1, t = 2$

v				
2	16	52	15	
1	8	62	14	
0	**37**	32	**51**	
	0	1	2	u

$w = 2, t = 2$

v				
2	25	10	**67**	
1	58	70	60	
0	0	**71**	4	
	0	1	2	u

$w = 0, t = 1$

v				
2	48	54	22	
1	56	55	12	
0	**77**	**11**	72	
	0	1	2	u

$w = 1, t = 1$

v				
2	**63**	**53**	**33**	
1	74	**47**	6	
0	28	**21**	45	
	0	1	2	u

$w = 2, t = 1$

v				
2	42	70	**39**	
1	2	**79**	30	
0	∞	**3**	**43**	
	0	1	2	u

$w = 0, t = 0$

v				
2	**29**	75	64	
1	78	**57**	**49**	
0	**1**	**59**	26	
	0	1	2	u

$w = 1, t = 0$

v				
2	38	**9**	**17**	
1	**69**	24	35	
0	**41**	66	**19**	
	0	1	2	u

$w = 2, t = 0$

This table was computed for the generator (of the multiplicative group) that is defined in the matrix representation of the field by the matrix

$$(A) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{pmatrix} .$$

The table of the field containing 81 elements is the geometric shorthand version of the $78 = 3^4 - 3$ identities:

$$A^0 = 1 \, , \; A^4 = 2A^3 + 1 \, , \; A^5 = A^3 + A + 2 \, ,$$

$$A^6 = 2A^3 + A^2 + 2A + 1 \, , \; A^7 = 2A^3 + 2A^2 + A + 2 \, , \; \ldots$$

$$\ldots \, , \; A^{79} = A^3 + A^2 \, , \; A^{80} = 1 \, .$$

All these identities follow recursively from the second one in this list (which is just the matrix (A) satisfying its characteristic equation).

The number of generators A^k of the multiplicative group (where $1 \leq k \leq 79$) equals $\varphi(3^4 - 1) = \varphi(5)\ \varphi(16) = 32$. These 32 values of the exponent k are shown in the table as bold characters.

The tables of the fields containing $2^5, 2^6$ and 2^7 elements have been published in the book: R. Lidl, H. Niederreiter, *Finite Fields*, second edition, Cambridge University Press, 1999 (on pages 673–676). This book also contains a large bibliography about the theory of finite fields and the proofs of the existence and uniqueness of the field containing p^n elements, as well as of the cyclicity of the multiplicative group of the field, which we have here omitted.

The tables of the fields containing 32, 64 and 128 elements are presented in this book for the choices of the multiplicative generators that are provided, respectively (in the matrix representation of the field), by the following three matrices:

$$(A) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} , \quad \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} , \quad \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} ,$$

implying, respectively, the characteristic equations encoded in the last line of these three Sylvester matrices:

$$A^5 = A^3 + 1 \, , \; A^6 = A^5 + 1 \, , \; A^7 = A + 1 \, .$$

Unfortunately, I do not know a convenient form for the generator A of the multiplicative group for a general field containing p^n elements, even for $p = 2$.

The reason for my ignorance might be the difficulty of the bibliographical search based on the book quoted above. It mentions, however, that many useful facts appeared first in the book: C.G.J. Jacobi, *Canon Arithmeticus*, Berlin, 1839, republished by Academic–Verlag, Berlin, in 1956.

However, this (apparently) full bibliography attributes the important general results of A. Girard (Amsterdam, 1629, 'Sur les découvertes nouvelles en algèbre'), which they use in their book, to I. Newton (1707) and to Waring.

Girard's forgotten theorem gives an expression for the moment function, which is the sum of the powers

$$s_k = x_1^k + \cdots + x_n^k$$

of the roots of the polynomial

$$\prod (x - x_j) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots \pm \sigma_n ,$$

in terms of the coefficients (predating the celebrated Chevalley theorem).

The expression is, of course, a polynomial with integral coefficients in the variables σ_j. These coefficients have many remarkable properties, relating them both to the natural sciences and to number theory, including some generalisations of 'Fermat's little theorem' to the traces of matrices.

The asymptotic behaviour of these coefficients gives a combinatorial definition of the entropy function $\sum p_j \log p_j$ (which describes the statistics of long words in a finite alphabet in terms of the frequencies p_j of occurrence of characters in these words).

The same coefficients also provide interesting extensions of the strange 'modular', or 'pseudo-doubly periodic' p-adic behaviour of the degree $d(a, b)$ of the prime p in the congruences

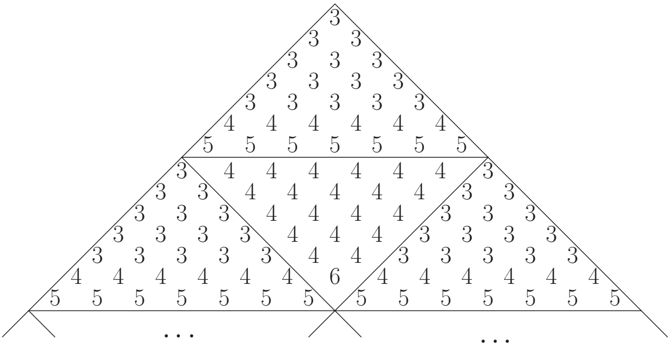
$$C_{pa}^{pb} - C_a^b = p^d q ,$$

where q is relatively prime to p, for the binomial coefficients and for their multinomial extension.

More details about these congruences and about the strange periodicities of the function d can be found in my article "Fermat dynamics of matrices, finite circles and finite Lobachevsky planes", Cahiers du CEREMADE, Université de Paris-Dauphine, No. 0434 (3 June 2004) and in the book "Arnold's Seminar Problems, 2004" published in Russian by MCCME, Moscow, 2005.

For instance, $d(mp + 1, b)$ does not depend on b when m is not too large and d satisfies some p-adic periodicity in both arguments a and b.

One might guess the nature of the function d of the two variables a and b by studying the following table of its values for $p = 7$, where the 14 rows of the Pascal-arranged triangle below correspond to the values $2 \leq a \leq 15$ of the arguments for the rows, and where $0 < b < a$ in each row:



```
                          3
                        3   3
                      3   3   3
                    3   3   3   3
                  3   3   3   3   3
                4   4   4   4   4   4
              5   5   5   5   5   5   5
            3   4   4   4   4   4   4   3
          3   3   4   4   4   4   4   3   3
        3   3   3   4   4   4   4   3   3   3
      3   3   3   3   4   4   4   3   3   3   3
    3   3   3   3   3   4   4   3   3   3   3   3
  4   4   4   4   4   4   6   4   4   4   4   4   4
5   5   5   5   5   5   5   5   5   5   5   5   5   5
        . . .                      . . .
```

The ‘double periodicity’ of this picture is only a finite repetition of the ‘fundamental domain’ of scale p, which is repeated p times in both directions. The subsequent repetition is disturbed by some corrections. The resulting block of scale p^2 is also repeated (p times in each direction) and is then disturbed to produce a further block of scale p^3, and so on. But despite this p-adic pseudo-periodicity and the appearance of p^n in the picture, neither the exact p-adic formula for this ‘periodicity’, nor its relation to the Galois fields of p^n elements is known.

The little Fermat theorem is related to the inequality $d \geq 2$ and to the irregular growth of $d(a, b)$ with a.

The matrix version of this theorem, or rather of its generalised form, discovered by Euler, $a^m \equiv a^{m-\varphi(m)} \pmod{m}$, is the congruence of the traces of integer matrices,

$$\operatorname{tr}(A^m) \equiv \operatorname{tr}\left(A^{m-\varphi(m)}\right) \pmod{m}$$

for $m = p^n$.

Some results in this direction are published in: V.I. Arnold. ‘On the matricial version of Fermat–Euler congruences’, *Japanese Journal of Mathematics*, **1** (2006) 1–24.

The relevance of the last condition for the validity of this congruence suggests its relation to Galois fields (but, as far as I know, such a relation has yet to be discovered).[†]

[†] The conjecture formulated in the paper quoted above has now been proved by P. Deligne. His proof is based on the relation to the theory of Galois fields suggested in my paper.

It is a pity that all these remarkable facts are neglected in modern mathematics and computer science. Numerical experiments helped a great deal in the discovery of the relevant empirical facts. For example, suppose the number of divisors of a large integer n grows with n, on average, like its natural logarithm $\ln n$. The sum of the average growth of the divisors is cn, where $c = \zeta(2) = \pi^2/6 \approx 3/2$. The mean average growth of the divisor is, however, $c_1 n/(\sqrt{\ln n})$, rather than $cn/\ln n$, as a scientist might suggest.

This last asymptotic result was discovered by A. Karazuba[†], following a lecture by me on Dirichlet's earlier results on averaged asymptotics. But no one knows the averages of the numbers of divisors τ of their sum σ and of the mean divisor σ/τ for the values of the Euler function taken as arguments of these functions – that is, for $\sigma(\varphi(n))/\tau(\varphi(n))$ – which would presumably explain the averaged asymptotics of the Euler period $T(n)$ (this being the minimal period of the geometric progression of the residues a^t $(t = 1, 2, \ldots, T)$ modulo n).

Empirically this asymptotic growth rate (Cesaro-averaged in n) is observed to be $c(a)n/(\ln n)$, as was computed by F. Aicardi[‡] for the situation when $n \lesssim 10^9$.

The minimal period $T(n)$ is a divisor of the value $\varphi(n)$ of the Euler function. If it really did differ in the average from the Cesaro-averaged growth rate of the mean divisor of $\varphi(n)$ (as the above empirical data suggest), then such a difference might be explained either by the fact that nature chooses for the period $T(n)$ a non-random divisor of $\varphi(n)$ which is far from its mean divisor; or alternatively by the fact that the number $\tau(m)$ of the divisors of $m = \varphi(n)$, their sum $\sigma(m)$ and the ratio $\sigma(m)/\tau(m)$ might behave (in the Cesaro average) very differently with the arguments $m = \varphi(n)$ than with the random arguments m.

Indeed it might happen that the values $\varphi(n)$ of the Euler function (for random choices of n) exhibit very different behaviour of the divisors

[†] The constant c_1 was then computed by M. Korolev to be $c_1 \approx 0.7138067\ldots$:

$$c_1 = \frac{1}{\pi} \prod_p \frac{p^{3/2}}{\sqrt{p-1}} \ln\left(1 + \frac{1}{p}\right) .$$

In the paper by P.T. Bateman, P. Erdős and C. Pommerance 'The arithmetic mean of the divisors of an integer', (Springer Lecture Notes in Mathematics, 1981, **899**, 197–220), the following result was given:

$$\sum_{n \le x} \frac{\sigma(n)}{\tau(n)} \sim \frac{g(1)x^2}{2\sqrt{\pi}\sqrt{\ln x}} \quad \text{for} \quad x \to \infty,$$

where, for Re $> \frac{1}{2}$, $g(s) = \prod_p (1 - \frac{1}{p^s}{}^{1/2}(1 + \frac{1}{2}(1 + \frac{1}{p})p^{-s} + \frac{1}{3}(1 + \frac{1}{p} + \frac{1}{p^2})p^{-2s} + \cdots)$.

[‡] *C.R. Acad. Sci., Paris, ser. I*, **339** (2004), 15–20: 'Empirical estimates of the average order of orbits period lengths in Euler groups'.

$\big(\tau(\varphi(n)), \sigma(\varphi(n)), \sigma(\varphi(n))/\tau(\varphi(n))\big)$, compared with that of the random numbers n themselves $\big(\tau(n), \sigma(n), \sigma(n)/\tau(n)\big)$.

These (alternative?) explanations for the non-randomness of the data of the average divisors of $\varphi(n)$ or of the special divisor $T(n)$ of $\varphi(n)$ are both possible.

To see whether they really occur requires both empirical study and mathematical theories. But these subjects seem to be too classical to attract modern mathematicians.

The unity of mathematics is its main jewel. I have hoped here to contribute to this unity by the geometric presentation of Galois fields and of its relation to the ergodic theory of dynamical systems, to statistics and to projective geometry, and also to returning all these forgotten classical theories to the continuous real ($\mathbb{R}$) world of the natural sciences.

Index