Diophantine Geometry and Dynamical Systems

Antoine Chambert-Loir

Irmar, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex, France
Courriel : antoine.chambert-loir@univ-rennes1.fr

Abstract. — Solving Diophantine equations, that is finding the solutions in rational integers of polynomial equations is one of the oldest task of mathematicians. During the 20th century, this subject has been geometrized so as to become what is now known as Diophantine Geometry.

A lot of questions have been asked, and many beautiful answers have been given, by mathematicians like Mordell, Weil, Manin, Mumford, Lang, Bogomolov, Faltings, Ullmo, Zhang... They mostly concern subvarieties of Abelian varieties, torsion points, or subgroups of finite rank. The notion of height often plays a crucial rôle.

Around 1990, notably under the impulse of Silverman, some of those questions have been broadened so as to replace Abelian varieties by Algebraic dynamical systems, namely algebraic varieties together with a self-map turning all of the old answers into totally open new questions.

In this talk, I shall brush a picture of this remarkable story.

1. Diophantine equations

Diophantine equations are polynomial equations where the unknowns are integers.

When the degree of the equations is 1, they are basically solved using the so called Chinese Remainder Theorem. Indeed, its first appearance can be found in an old text (III-V$^{\text{th}}$ century A.D., the precise date is unknown) by Sūnzǐ, called the Sūnzǐ Suàngjīng 孫子算經, "The mathematical classic of Sūnzǐ": (see Fig. 1):

有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物几何？

which translates as:

> Now there are an unknown number of things. If we count by threes, there is a remainder 2; if we count by fives, there is a remainder 3; if we count by sevens, there is a remainder 2. Find the number of things. — *Translation from Lam & Ang (2004)*

This kind of exercise has been reprinted in later mathematical manuals, such as the 1247 Shùshū Jiǔzhāng (數書九章, *Mathematical Treatise in Nine Sections*), itself included in the XIXth century's Sìkù quánshū (四庫全書, The Complete Library of the Four Treasures, see Fig. **??**), a kind of encyclopaedia commissioned by the Qing emperors to show they could surpass the Ming's Encyclopaedia (from 1403 A.D.). Its modern mathematical formulation would be (the main unknown is n)

$$n = 3x + 2 = 5y + 3 = 7z + 2,$$

whose smallest positive solution is $n = 23$.

In degree 2, the most prominent example is probably the *Pell equation* $x^2 - ny^2 = 1$, the unknowns being x and y, and n being a non-zero parameter which is not a square. In fact, this equation was first studied by the Indian mathematician Brahmagupta (628 A.D.) who already observed that from two solutions (x, y) and (x', y'), one could define a third one (x'', y''), given by

$$x'' = xx' + nyy', \quad y'' = xy' + x'y.$$

This relation is better understood if one writes $x^2 - ny^2 = (x+\sqrt{n}y)(x-\sqrt{n}y)$ as the *norm* of $x+\sqrt{n}y$, and observes that

$$(x+\sqrt{n}y)(x'+\sqrt{n}y') = (xx'+nyy') + \sqrt{n}(xy'+x'y).$$

In fact, all solutions can (up to sign) be constructed by this process from a single, minimal, one. This equation also intervenes in the solution to Archimedes's cattle problem (III$^{\text{rd}}$ century B.C., Fig. 3).

The study of equations of degree 3 or more is much more recent. One must of course quote Fermat's "*Last Theorem*", staten in 1637 and first proven by Andrew Wiles (partly with Richard Taylor) in 1995. Fermat was in fact studying the works of Diophantus of Alexandria who solved the quadratic equation in three integer variables a, b, c,

$$a^2 + b^2 = c^2,$$

whose solutions give the possible triangles having a right angle and sides with integer lengths. In the margin of his own edition (see Fig. 4 for a later edition incorporating Fermat's comments), Fermat claimed to have proven that similar higher degrees equations,

$$a^3 + b^3 = c^3, \quad a^4 + b^4 = c^4, \dots$$

have no solutions besides the obvious ones where one of the variable is zero. Although mathematicians like Fermat himself, Euler, Sophie Germain, Kummer,... proved many cases, the full proof of this statement had to await much more modern tools.

In his proof of the quartic case, Fermat invented the method of *infinite descent*. Assuming there is a nontrivial solution (a, b, c) of equation $a^4 + b^4 = c^4$ and consider the smallest one (one for which, say, c is minimal), he used the parametrization of solutions of the quadratic equation $A^2 + B^2 = C^2$ to construct a smaller solution. This is a contradiction which proves that there are no nontrivial solutions.

In fact, it is simpler to show that the equation $a^4 + b^4 = c^2$ has only trivial solutions. So take a, b, c positive integers such that $a^4 + b^4 = c^2$, with c minimal. Necessarily a, b, c are coprime; set $A = a^2$, $B = b^2$, $C = c$. One has $A^2 + B^2 = C^2$ hence (assuming that A is odd and B is even, which is possible, up to exchanging a and b), there are coprime integers U and V, such that

$$A = U^2 - V^2, \quad B = 2UV, \quad C = U^2 + V^2.$$

In other words,

$$a^2 + V^2 = U^2, \quad b^2 = 2UV, \quad c = U^2 + V^2.$$

Looking modulo 4, we see that V is even and U is odd. Since U and V are coprime and $b^2 = 2UV$, there are integers u and v such that $U = u^2$ and $V = 2v^2$; then, $b = 2uv$. From the equation $a^2 + V^2 = U^2$, we see that there are coprime integers X, Y such that $a = X^2 - Y^2$, $V = 2XY$, $U = X^2 + Y^2$. Then $v^2 = XY$ and, X and Y being coprime, they both must be squares: $X = x^2$, $Y = y^2$. Finally, we get $U = u^2 = x^4 + y^4$ which is an equation of the same form as the one studied. Moreover, one checks that $c = U^2 + V^2 > U^2 \geqslant U$, which contradicts the minimality of c.

2. Birth of Diophantine geometry: curves and abelian varieties

During the XIX$^{\text{th}}$ century, the geometry of algebraic curves and abelian varieties has emerged from complex analysis under the hands of Riemann, Jacobi, Abel, and others.

Concerning curves, it was understood that the degree of a plane curve does not fully reflect its geometry, unless the curve is without singularities. The *genus* is a better invariant. In that respect, equations of degree 1 or 2 furnished curves of genus 0; equations of degree 3 or more tend to give curves of higher genus.

Elliptic curves are curves of genus one, together with a point o on it. Over the complex numbers, such a curve (X, o) has a cubic plane equation of Weierstrass's form, namely

$$y^2 = x^3 = ax + b$$

(in the affine plane; homogeneize to get the projective equation), the point o being the point at infinity. It can be parametrized via Weierstrass's $\wp$-function: there exists a lattice $\Lambda \in \mathbf{C}$ such that the map

$$z \mapsto (\wp(z), \wp'(z)), \qquad \wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

is Λ-periodic and induces an isomorphism $\mathbf{C}/\Lambda \xrightarrow{\sim} X$. Observe that this parametrization endows X with a structure of an Abelian group, the point o being the origin. In fact, this group structure has a well-known geometric construction: take two points (x, y) and (x', y'); the line through them intersects the curve in a third point (x'', y''), the symmetric of which with respect to the x-axis is the sum of the two points (x, y) and (x', y').

The question of finding rational (resp. integer) solutions to such cubic Weierstrass's equations is therefore expressed as finding rational points on elliptic curves (resp. integral points on $X \setminus \{o\}$).

The results are as follows:

Theorem 2.1. — *Let X be an elliptic curve given by a Weierstrass equation with coefficients in a number field F.*

The set of rational points of X is an Abelian group of finite type (Mordell (1922); Weil (1929)).

The set of integral points of $X \setminus o$ is finite (Siegel (1929))

In higher genus, the following result had been conjectured by Mordell.

Theorem 2.2. — *Let X be an algebraic curve of genus $g \geqslant 2$ defined over a number field. Then the set of rational points of X is finite (Faltings (1983)).*

Vojta (1991) gave another proof which was subsequently simplified by Bombieri (1990). That proof inspired Faltings (1991) to give the proof of a more general conjecture of Serge Lang.

On the circle with equation $x^2 + y^2 = 1$, the indefinite integral of the differential form $\mathrm{d}y/x = \mathrm{d}y/\sqrt{1-y^2}$ leads to trigonometrical functions and their functional equations. The XIX$^{\text{th}}$-century geometers understood how this phenomenon generalizes in higher genus. First of all, on a compact Riemann surface X of genus g, there are exactly g independent differential forms, say $\omega_1, \ldots, \omega_g$. Fixing a base point $o \in X$, they lead to indefinite integrals, $P \mapsto \int_o^P \omega_j$, which however are only well-defined up to the integrals over closed loops. This furnishes a map from X to the quotient of the space $\mathbf{C}^g$ by a lattice Λ, consisting of all $(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g)$, where γ ranges over the first homology group of X. This variety $JX = \mathbf{C}^g/\Lambda$ is called the Jacobian variety of X, and the map $X \to JX$ is an embedding (if $g \geqslant 2$), an isomorphism if $g = 1$.

Weil gave an algebraic description of this Jacobian variety. When X is defined over a number field, so is JX, hence one can talk about the rational points of JX. The following result of Weil applies in fact to a broader class of varieties, called *abelian varieties*: these are projective varieties endowed with a structure of group whose law is given by regular algebraic functions. In dimension 1, we find elliptic curves again; in higher dimension, we have Jacobian varieties but they don't exhaust the multiplicity of abelian varieties.

***Theorem 2.3* (Mordell-Weil Theorem).** — *Let A be an abelian variety defined over a number field. Then its set of rational points is an Abelian group of finite type (Weil (1929)).*

This is a generalization of the previous theorem for elliptic curves. Many questions remain on that topic, the most obvious being the conjecture of Birch and Swinnerton-Dyer, which gives an analytic formula for the rank of this Abelian group. Except in some important cases (elliptic curves over $\mathbf{Q}$,... according to the fundamental results of Wiles, Taylor and others) this formula expresses the rank as the order of the zero of an analytic function at $s = 1$, while this function is defined by a Dirichlet series which is only known to converge for $\Re(s) > 3/2$!

Faltings's generalization of Mordell's conjecture alluded to above is the following:

Theorem 2.4. — *Let X be a subvariety of an abelian variety defined over a number field. The set of translates of abelian subvarieties of positive dimension contained in X has finitely many maximal elements. Let X^* be X deprived of these translates; unless X is itself a translate of an abelian variety, X^* is non-empty. Then, X^* has only finitely many rational points (Faltings (1991)).*

If X is a curve of genus $g \geqslant 2$ embedded in its Jacobian variety JX, one has $X^* = X$, so that that X has only finitely many rational points. On the opposite, the hypothesis of the Theorem is necessary: if B is a subabelian variety of positive dimension of A, then up to enlarging the ground field, B has potentially infinitely many rational points.

In fact, the more general "Mordell–Lang conjecture" is true:

Theorem 2.5. — *Let X be a subvariety of an abelian variety A. Let X^* be X deprived of these translates; unless X is itself a translate of an abelian variety, X^* is non-empty. Any subgroup Γ of A which is finitely generated intersects X^* in a finite set.*

(This follows from an extension of Faltings's theorem where one allows finitely generated, possibly nonalgebraic, extensions of $\mathbf{Q}$.)

3. Geometrizing the infinite descent: heights

All proofs of the theorems quoted above make a crucial use of the notion of height.

The height of a rational number $\alpha = m/n$ is defined as $h(\alpha) = \log\max(|m|, |n|)$, provided the fraction m/n is in lowest terms. There are finitely many rational numbers of height bounded from above by any prescribed constant.

Let us consider points of the projective space $\mathbf{P}^d$ of dimension d; such a point P has homogeneous coordinates $(x_0 : \ldots : x_d)$, not all zero and well defined up to multiplication by a common scalar. If F is a field (containing $\mathbf{Q}$), one says that P is F-rational if it admits a system of homogeneous coordinates in F; equivalently, if the ratii x_j/x_i (for $x_i \neq 0$) all belong to F. One writes $\mathbf{P}^d(F)$ for the set of F-rational points of $\mathbf{P}^d$; one writes also $\mathbf{Q}(P)$ for the field generated by the ratioi x_j/x_i over $\mathbf{Q}$ and call it the *field of definition of P*.

To begin with, let $P \in \mathbf{P}^d(\mathbf{Q})$; let us consider a system of homogeneous coordinates $(x_0 : \ldots : x_d)$ for P, consisting of rational numbers. We can first chase the denominators and assume that all the x_j are integers; then we can divide by their gcd and assume moreover that these integers are coprime. Only one more possibility is left, namely multiplying the system by -1. In any case the real number

$$h(P) = \log\max(|x_0|, \ldots, |x_d|), \qquad (x_0, \ldots, x_d) \text{ coprime integers}$$

is well-defined; we call it the height of the point P. Again, there are finitely many $\mathbf{Q}$-rational points of $\mathbf{P}^d$ whose height are bounded from above by any prescribed constant.

The definition can be generalised to all points in $\mathbf{P}^d(\overline{\mathbf{Q}})$, where $\overline{\mathbf{Q}}$ is the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. There are many ways (all equivalent) to define $h(P)$; for example, one may choose a system

of homogeneous coordinates $(x_0 : \ldots : x_d)$ consisting of algebraic integers which generate, as an ideal, the ring of all algebraic integers. Then,

$$h(P) = \frac{1}{[\mathbf{Q}(x_0,\ldots,x_d) : \mathbf{Q}]} \sum_{\sigma : \mathbf{Q}(P) \hookrightarrow \mathbf{C}} \log \max(|\sigma(x_0)|, \ldots, |\sigma(x_d)|), \qquad \text{if } \sum x_j \overline{\mathbf{Z}} = \overline{\mathbf{Z}},$$

where the sum runs over the field embeddings σ of $\mathbf{Q}(P)$ into the field $\mathbf{C}$ of complex numbers.

When $d = 1$, $P = (1 : \alpha)$, then $h(P)$ is related to the Mahler measure $\mathrm{M}(\Pi_\alpha)$ of the minimal polynomial Π_α of α:

$$h(P) = \frac{1}{[\mathbf{Q}(\alpha) : \mathbf{Q})]} \mathrm{M}(\Pi_\alpha) = \int_0^1 \log(\left|\Pi_\alpha(e^{2i\pi t})\right|) \, \mathrm{d}t.$$

One of the geometric contents of this height function lies in its functorial properties:

Proposition 3.1. — *Let X be a closed subvariety of a projective space $\mathbf{P}^n$, defined over the field of algebraic number and let $f : X \to \mathbf{P}^m$ be a morphism from X to $\mathbf{P}^m$ given by forms of degree d which have no common zero on X. Then there exists a real number c such that, for any point $P \in X(\overline{\mathbf{Q}})$,*

$$d\,h(P) - c \leqslant h(f(P)) \leqslant d\,h(P) + c.$$

(The upper bound is relatively obvious, the lower bound depends on Hilbert's *Nullstellensatz*.)

This has application to abelian varieties: since the addition law can be written with quadratic equations, one can prove that for any abelian variety X, there exist a quadratic form q and a linear form ℓ on the group $X(\overline{\mathbf{Q}})$, and a real number c, such that for any point $P \in X(\overline{\mathbf{Q}})$,

$$q(P) + \ell(P) - c \leqslant h(P) \leqslant q(P) + \ell(P) + c.$$

For "symmetric embeddings", the linear form ℓ vanishes and the quadratic form q is called the Néron-Tate height of the point P. It has been constructed by Néron (1965) via a difficult and profound analysis; a straightforward proof has soonafter been given by John Tate—we shall return on this.

Moreover, the height satisfies an easy, but crucial, boundedness property:

Theorem 3.2. — *For any real number B and any integer d, there are only finitely many points $P \in \mathbf{P}^n(\overline{\mathbf{Q}})$ such that $[\mathbf{Q}(P) : \mathbf{Q}] \leqslant d$ and $h(P) \leqslant B$ (Northcott (1950)).*

If X is an abelian variety, one can use this boundedness property to deduce the corollary, which characterizes torsion points in $X(\overline{\mathbf{Q}})$ in terms of their heights:

Corollary 3.3. — *Let X be an abelian variety defined over the field of algebraic numbers. A point $P \in X(\overline{\mathbf{Q}})$ is a torsion point if and only if its Néron-Tate height vanishes.*

Let us say explan how heights are used to prove the Mordell-Weil Theorem (Theorem 2.3). The points P in $A(\overline{\mathbf{Q}})$ such that $2P = 0$ form a finite subgroup A_2. One may assume that F is large enough so that all of these points are defined over F.

First of all, one proves that *the group $A(F)/2A(F)$ is finite*. This is done nowadays by observing that for any point $P \in A(F)$, the points $Q \in A(\overline{\mathbf{Q}})$ such that $2Q = P$ are defined over an extension of F of degree $\leqslant 4^g$ which is unramified outside a fixed set of places of F. By an important theorem of Hermite, the set of such fields is finite, so that there is a finite Galois extension F' of F, independent of P, such that $Q \in A(F')$. Now, given $P \in A(F)$, define $c(P)$ to be the map from $\mathrm{Gal}(F'/F)$ to $A(F')$ given by $c(P)_\sigma = \sigma(Q) - Q$, where $Q \in A(F')$ is any chosen point such that $2Q = P$ (this does not depend on the choice of Q). Observe that

$2c(P)_\sigma = \sigma(2Q) = 2Q = \sigma(P) - P = 0$, so that the image of $c(P)$ lies within the finite set of points of $A(\overline{\mathbf{Q}})$ whose order divides 2. Moreover, if $P \in 2A(F)$, then $c(P) = 0$ (choose Q such that $P = 2Q$); conversely, if $c(P) = 0$, then the chosen point Q satisfies $\sigma(Q) = Q$ for all $\sigma \in \mathrm{Gal}(F'/F)$, hence $Q \in A(F)$. The map c is linear in P; it induces an injective morphism of Abelian groups from $A(F)/2A(F)$ to the finite group $\mathrm{Hom}(\mathrm{Gal}(F'/F), A_2)$. So $A(F)/2A(F)$ is finite.

Then, one uses heights and descent. Take a finite system of representatives $(P_1, \dots, P_m)$ for $A(F)/2A(F)$ and consider $Q \in A(F)$. One may write it $Q = \sum a_i P_i + 2Q_1$, with $a_i \in \{0,1\}$ and $Q_1 \in A(F)$. Using the fact that the Néron-Tate height $\hat{h}$ is a quadratic form, one gets

$$\hat{h}(Q_1) = \frac{1}{4}\hat{h}(Q - \sum a_i P_i) \leqslant \frac{1}{4}\hat{h}(Q - \sum a_i P_i) + \frac{1}{4}\hat{h}(Q + \sum a_i P_i) = \frac{1}{2}\hat{h}(Q) + \frac{1}{2}\hat{h}(\sum a_i P_i) \leqslant \frac{1}{2}\hat{h}(Q) + c,$$

where c is the maximum of all heights $\hat{h}(\sum a_i P_i)$, when $(a_1, \dots, a_m)$ varies among $\{0,1\}$. if $\hat{h}(Q) > c$, then one obtains $\hat{h}(Q_1) < \hat{h}(Q)$.

Go on from Q_1 with the same process, defining Q_2,..., as long as the height decreases. The sequence obtained must stop eventually, because of Northcott's finiteness theorem, and reach a point Q_n such that $\hat{h}(Q_n) \leqslant c$, and the point Q can be written as a linear combination of $P_1, \dots, P_m$ and Q_n. By Northcott's theorem again, there are finitely many points in $A(F)$ whose heights are less than c, so that Q_n belongs to a fixed finite set. In other words, $A(F)$ is generated by the union of the set $\{P_1, \dots, P_m\}$ and of the set of points with heights $\leqslant c$.

4. The conjectures of Manin–Mumford of Bogomolov

Motivated by Mordell's conjecture and its generalization to subvarieties of abelian varieties, Manin and Mumford conjectured the following statement, now a theorem of Raynaud.

Theorem 4.1 **(Raynaud (1983*a*,*b*)).** — *Let X be a subvariety of an Abelian variety A. Let X° be the complement in X of all translates of positive dimensional abelian subvarieties of A by a torsion point which are contained in X. Then, X° is an open subset of X for the Zariski topology and contains only finitely many torsion points of A.*

That X° is open means that there is a finite set $Y_1, \dots, Y_m$ of translates of positive dimensional abelian subvarieties of A by torsion points which are contained in X and whose union contains any such variety. If X itself is not a translate of an abelian subvariety of A by a torsion point, then X° is non-empty.

Here is an alternate formulation: if X contains a dense set of torsion points, then X is the translate of an abelian subvariety by a torsion point.

Recall that torsion points are points of Néron-Tate height 0. Still motivated by Mordell's conjecture, Bogomolov put forward the following statement, now a theorem of Ullmo and Zhang:

Theorem 4.2 **(Ullmo (1998); Zhang (1998)).** — *Let X be a subvariety of an Abelian variety A over a number field. Let X° be X deprived of all translates of positive dimensional abelian subvarieties of A by a torsion point which are contained in X. Then there exists a positive real number δ_X such that for any point $P \in X^\circ(\overline{\mathbf{Q}})$ which is not a torsion point, $\hat{h}(P) \geqslant \delta_X$.*

(In fact, Ullmo and Zhang's proof provides a new proof of Raynaud's theorem, which is not apparent in the statement I just gave.)

The proof of this theorem relies on an *equidistribution property*. Let F be a number field over which A is defined. Let P be any point $P \in A(\overline{\mathbf{Q}})$. Since its field of definition $\mathbf{Q}(P)$ is a number field, the point P has finitely many conjugates; equivalently, the orbit of P under the action of $\mathrm{Gal}(\overline{F}/F)$ is finite; let $P_1, \dots, P_m$ be those conjugates (with $m = [F(P) : F]$) and define

the probability measure $\delta(P)$ as the discrete measure on $A(\mathbf{C})$ which gives every point P_j the mass $1/m$.

For any subvariety X of A, the space $X(\mathbf{C})$ carries a natural positive probability measure μ_X. When $X = A$, μ_X is the normalized Haar measure on $A(\mathbf{C})$. The measures μ_X are defined by complex geometry: if $A(\mathbf{C}) = \mathbf{C}^g/\Lambda$ (where Λ is some lattice), let ω be a Riemann form of Λ; this is an Hermitian form on $\mathbf{C}^g$ (associated to some polarization) which we view as differential form

$$\omega = \sum \omega_{i,j} \mathrm{d}z_i \wedge \mathrm{d}\overline{z}_j$$

on $A(\mathbf{C})$. Then, if $d = \dim(X)$, the restriction of ω^d to the smooth locus of $X(\mathbf{C})$ is a positive volume form of finite total mass; μ_X is the unique probability measure which is proportional to $\omega^2|_X$.

***Theorem 4.3* (Szpiro *et al* (1997)).** — *Let X be a subvariety of A. Let (P_j) be a sequence of points in $X(\overline{\mathbf{Q}})$ which satisfies the following properties:*

(1) *when $j \to \infty$, $\hat{h}(P_j) \to 0$;*

(2) *for any subvariety $Y \subsetneq X$, the set of indices j such that $P_j \in Y$ is finite.*

Then, the measures $\mu(P_j)$ converge to μ_X.

Given the equidistribution theorem, the proofs of Ullmo and Zhang are truly marvelous. Let's assume, for simplicity, that X is a curve of genus g in its Jacobian embedding and that $g \geqslant 2$, so that $X^\circ = X$. From the sequence (P_j), Ullmo defines a sequence (Q_k) of points in $X^g(\overline{\mathbf{Q}})$ which satisfy the hypotheses of the equidistribution theorem, X^g being seen as a subvariety of A^g. (Each point Q_k is of the form $(P_{j_1}, \dots, P_{j_g})$.) Therefore, the measures $\mu(Q_j)$ converge to the measure μ_X^g on $X^g(\mathbf{C})$.

Moreover, Ullmo considers the addition map $\sigma\colon A^g \to A$. It is well known that the restriction of the addition map to X^g is generically finite-to-one and that $\sigma(X^g) = A$. Moreover, the quadratic property of the Néron-Tate height imply that $\hat{h}(\sigma(Q_j))$ converge to 0 when $k \to \infty$. Consequently, the sequence $(\sigma(Q_k))$ also satisfies the equidistribution theorem and the measures $\mu(\sigma(Q_k))$ converge to $\mu_{\sigma(X^g)} = \mu_A$.

Now comes the contradiction: for any point $Q \in X^g(\mathbf{C})$, the measure $\mu(\sigma(Q))$ is equal to the measure $\sigma_*\mu(Q)$ obtained by pushing forward the measure $\mu(Q)$ by σ. By continuity, $\sigma_*(\mu_X^g) = \mu_A$. Looking at this equality of measures at points where σ is an étale map, we deduce an equality of differential forms $\sigma^*\mu_A = g!\mu_X^g$, where $g!$ is the degree of σ. But this equality is absurd. Indeed, μ_X is a volume form which is positive everywhere on $X(\mathbf{C})$, and so is μ_X^g. However, $\sigma^*\mu_A$ vanishes where σ is not étale, for example along the diagonal of X^g where its tangent map has rank 1.

5. Dynamical systems

We have seen that the self-map of an abelian variety given by multiplication by 2 has been playing an important rôle for its arithmetic. This brought J. Silverman to suggest studying the arithmetic properties of algebraic varieties endowed with self-maps. This theory is now a full mathematical subject, whose basics (and beyond) are exposed in the book (Silverman, 2007).

In fact, the question had been posed as early as 1950, for this was the main topic of the mentioned paper of Northcott!

So let X be a projective variety and let $f\colon X \to X$ be a self-map, given in some projective embedding by polynomials of degree d, without common zeroes on X. Anyway, we now view

our (X, f) as a *dynamical system*. Given a point P on X, one can look at its forward-orbit $(P, f(P), f^2(P), \dots)$. We can also consider backward-orbits, namely sequences $(\dots, P_1, P_0)$ of points in X such that $f(P_j) = P_{j-1}$ for any $j \geqslant 1$. In this setting, one says that a point P is *periodic* if there exists a positive integer n such that $f^n(P) = P$; and that it is *preperiodic* if there exist two integers m and n, with $n > m$, such that $f^n(P) = f^m(P)$ — this is equivalent to asking that the forward-orbit be finite. The integer d is called the *dynamical degree* of (X, f).

For example, one could take for (X, f) an abelian variety and its multiplication-by-2 map. In that case, I let as an exercise to prove that preperiodic points are precisely the torsion points! Another example is given by taking $X = \mathbf{P}^1$ (the projective line) and for f any rational function $f \in \overline{\mathbf{Q}}(T)$. It is useful to develop this theory in a more general setting, to include into the picture some automorphisms of certain K3-surfaces, as in (Silverman, 1991), but this would bring us too far.

Let us assume that X and f are defined over the field of algebraic numbers. Then we can look at heights and we see that there exists a real number c such that

$$d\,h(P) - c \leqslant h(f(P)) \leqslant d\,h(P) + c$$

for any point $P \in X(\overline{\mathbf{Q}})$. From that property, Northcott derived the following consequence:

***Theorem 5.1* (Northcott (1950)).** — *Assume that $d \geqslant 2$. Then, for any integer e, there are only finitely many points $P \in X(\overline{\mathbf{Q}})$ which are preperiodic for f and are defined over a field of degree less than e.*

Before we explain the proof, it is interesting to develop the heights-argument further.

***Proposition 5.2* (Call & Silverman (1993)).** — *Let us assume that X and f are defined over the field of algebraic numbers. There exists a unique function $\hat{h}$ on $X(\overline{\mathbf{Q}})$ satisfying:*

(1) *the function $\hat{h} - h$ is uniformly bounded on $X(\overline{\mathbf{Q}})$;*

(2) *for any $P \in X(\overline{\mathbf{Q}})$, $\hat{h}(f(P)) = d\hat{h}(P)$.*

This function $\hat{h}$ is called the canonical height.

The proof of the proposition follows closely Tate's proof of the existence of the Néron-Tate height: for any $P \in X(\overline{\mathbf{Q}})$, prove that when $n \to \infty$, $h(f^n(P))/d^n$ converges to a limit, call it $\hat{h}(P)$, and show that the function $\hat{f}$ so-defined is the unique function which satisfies the two requirements of the proposition.

Now, it is a simple matter to prove that the canonical height is nonnegative (just use the limit formula, using the fact that by definition the height is bounded from below), and that preperiodic points are exactly points of canonical height zero. Indeed, if $f^n(P) = f^m(P)$ with $n > m$, then

$$d^n \hat{h}(P) = \hat{h}(f^n(P)) = \hat{h}(f^m(P)) = d^m \hat{h}(P),$$

so $\hat{h}(P) = 0$ since $d^n \neq d^m$ (we use $d \neq 1$). Conversely, if $\hat{h}(P) = 0$, then all points in the forward-orbit $P, f(P), \dots$ have canonical height zero, so their usual heights are bounded. Since they are all defined over a common number field, the finiteness theorem implies that this forward-orbit is finite.

Theorem 5.1 also follows from the finiteness theorem, applied to the set of preperiodic points.

But apart from that, many questions and conjectures remain.

What is the analogue of Manin-Mumford conjecture? Namely, let X° be X deprived of all subvarieties of positive dimension Y which are preperiodic (that is, for which there exists m

and n such that $n > m$ and $f^n(Y) = f^m(Y)$). Is it true that X° is Zariski open in X and contains only finitely many preperiodic points?

This would be an analogue of Manin-Mumford's conjecture because in the case of Abelian varieties, the preperiodic subvarieties are exactly the translates of abelian subvarieties by torsion points.

Although Zhang (1995) had conjectured that the answer the preceding question is positive, Ghioca and Tucker discovered a simple counterexample in 2009. It is given as follows. Let $E = \mathbf{C}/\mathbf{Z}[i]$ be "the" elliptic curve with complex multiplication by $\mathbf{Z}[i]$ and let $X = E^2$, with the self map given by $f(x,y) = (5x, (3+4i)y)$. It has dynamical degree $5^2 = 3^2 + 4^2$.

One can check that preperiodic points of this dynamical system are pairs (x,y) of torsion points.

The tangent map to f has a diagonal matrix, with eigenvalues 5 and $3+4i$ whose quotient is not a root of unity. Except horizontal or vertical lines, no line is invariant under any non-trivial power of f. This implies that the preperiodic subvarieties are the vertical or horizontal curves, of the form $\{x\} \times E$ and $E \times \{y\}$, where x and y are preperiodic points. However, their union is not a Zariski closed subset of $E \times E$.

Alternatively, the diagonal Δ in $E \times E$ carries infinitely many preperiodic points (so a dense set of this since it has dimension 1) but is not itself preperiodic.

Recent work of Ghioca, Tucker and Zhang aims proposed a (possibly correct) version of a dynamical Manin-Mumford conjecture.

Anyway, Xiniyi Yuan has recently shown an analogue of the equidistribution theorem. To state it, I need to recall one fact from complex dynamical systems.

***Theorem 5.3* (Yuan (2008)).** — *Let (X,f) be an algebraic dynamical system of dynamical degree $\geqslant 2$, defined over the field of algebraic numbers, and let $\hat{h}$ be the canonical height. Let (P_j) be a sequence of points in $X(\overline{\mathbf{Q}})$ satisfying:*

(1) *when $j \to \infty$, $\hat{h}(P_j) \to 0$;*

(2) *for any subvariety $Y \subsetneq X$, the set of indices j such that $P_j \in Y$ is finite.*

Then, the measures $\delta(P_j)$ converge to the equilibrium probability measure $\mu_{X,f}$ on $X(\mathbf{C})$.

This equilibrium measure has been introduced by mathematicians in complex dynamics (Brolin, Lyubich, Hubbard-Papadopol, Dinh-Sibony) and can be defined as follows: take any smooth volume form ν on $X(\mathbf{C})$ and consider the sequence (ν_n) of forms given by $\nu_n = d^{-n\dim(X)}(f^n)^*\nu$. Then, $\nu_n \to \mu_{X,f}$ when $n \to \infty$.

This measure is very complicated in general. In fact, generalizing earlier work of Berteloot, Dupont, and Loeb, Cantat (2008) showed that $\mu_{X,f}$ is orthogonal to the Lebesgue measure, unless (X,f) is "built" from abelian varieties.

Backward orbits furnish a natural way to define sequences of points (P_j) as in the Theorem. Indeed, one has $\hat{h}(P_j) = d^{-j}\hat{h}(P)$. So Yuan's theorem implies that, provided no subsequence of (P_j) is contained in some strict subvariety of X, the measures $\delta(P_j)$ converge to μ_X.

However, nobody found yet how to use this equidistribution theorem to derive geometric results in the spirit of the Manin-Mumford conjecture.

There are other questions worth to be described, like the dynamical Mordell-Lang conjecture (for which many interesting papers were written in the recent years).

In recent years, there has been much activity about refinements of the Mordell-Lang conjecture. The keywords are "anomalous intersections" and new developments concern dynamical systems. (See Chambert-Loir (2011) for a survey on that topic.)

But also about the generalization to abelian varieties and dynamical systems of the theorem of Merel (1996) according to which, for any elliptic curve A defined over a number field, the cardinality of the torsion subgroup of $A(F)$ is bounded in terms solely of the degree of F.

However, it is time to stop. I refer the interested reader to a long survey of mine on this theme, namely interaction of Diophantine geometry, heights and dynamical systems, see Chambert-Loir (2010).

References

E. BOMBIERI (1990), "The Mordell conjecture revisited". *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, **17** (4), p. 615–640.

G. CALL & J. SILVERMAN (1993), "Canonical heights on varieties with morphisms". *Compositio Math.*, **89**, p. 163–205.

S. CANTAT (2008), "Caractérisation des exemples de Lattès et de Kummer". *Compos. Math.*, **144** (5), p. 1235–1270.

A. CHAMBERT-LOIR (2010), *Théorèmes d'équidistribution pour les systèmes dynamiques d'origine arithmétique*, Panoramas et synthèses **30**, p. 97–189. ArXiv:0812.0944.

A. CHAMBERT-LOIR (2011), "Relations de dépendance et intersections exceptionnelles". *Astérisque*. Séminaire Bourbaki, Vol. 2010/2011, Exposé 1032, to appear. ArXiv:1011.4738.

G. FALTINGS (1983), "Endlichkeitsätze für abelsche Varietäten über Zahlkörpern". *Invent. Math.*, **73** (3), p. 349–366.

G. FALTINGS (1991), "Diophantine approximation on abelian varieties". *Ann. of Math.*, **133**, p. 549–576.

L. Y. LAM & T. S. ANG (2004), *Fleeting footsteps. Tracing the conception of arithmetic and algebra in ancient China*, World Scientific Publishing Co. Inc., River Edge, NJ, revised edition. With a foreword by Joseph W. Dauben.

L. MEREL (1996), "Bornes pour la torsion des courbes elliptiques sur les corps de nombres". *Invent. Math.*, **124** (1-3), p. 437–449.

L. J. MORDELL (1922), "On the rational solutions of the indeterminate equations of the third and fourth degrees." *Cambr. Phil. Soc. Proc.*, **21**, p. 179–192.

A. NÉRON (1965), "Quasi-fonctions et hauteurs sur les variétés abéliennes". *Ann. of Math. (2)*, **82**, p. 249–331.

D. G. NORTHCOTT (1950), "Periodic points on an algebraic variety". *Ann. of Math.*, **51**, p. 167–177.

M. RAYNAUD (1983*a*), "Courbes sur une variété abélienne et points de torsion". *Invent. Math.*, **71** (1), p. 207–233.

M. RAYNAUD (1983*b*), "Sous-variétés d'une variété abélienne et points de torsion". *Arithmetic and Geometry. Papers dedicated to I.R. Shafarevich*, edited by M. ARTIN & J. TATE, Progr. Math. **35**, p. 327–352, Birkhäuser.

C. L. SIEGEL (1929), "Über einige Anwendungen diophantischer Approximationen." *Abh. Preuss. Akad. Wiss. Phys.-Math.*, **1**, p. 209–266.

J. H. SILVERMAN (1991), "Rational points on $K3$ surfaces: a new canonical height". *Invent. Math.*, **105** (2), p. 347–373.

J. H. SILVERMAN (2007), *The arithmetic of dynamical systems*, Graduate Texts in Mathematics **241**, Springer, New York.

L. SZPIRO, E. ULLMO & S.-W. ZHANG (1997), "Équidistribution des petits points". *Invent. Math.*, **127**, p. 337–348.

E. ULLMO (1998), "Positivité et discrétion des points algébriques des courbes". *Ann. of Math.*, **147** (1), p. 167–179.

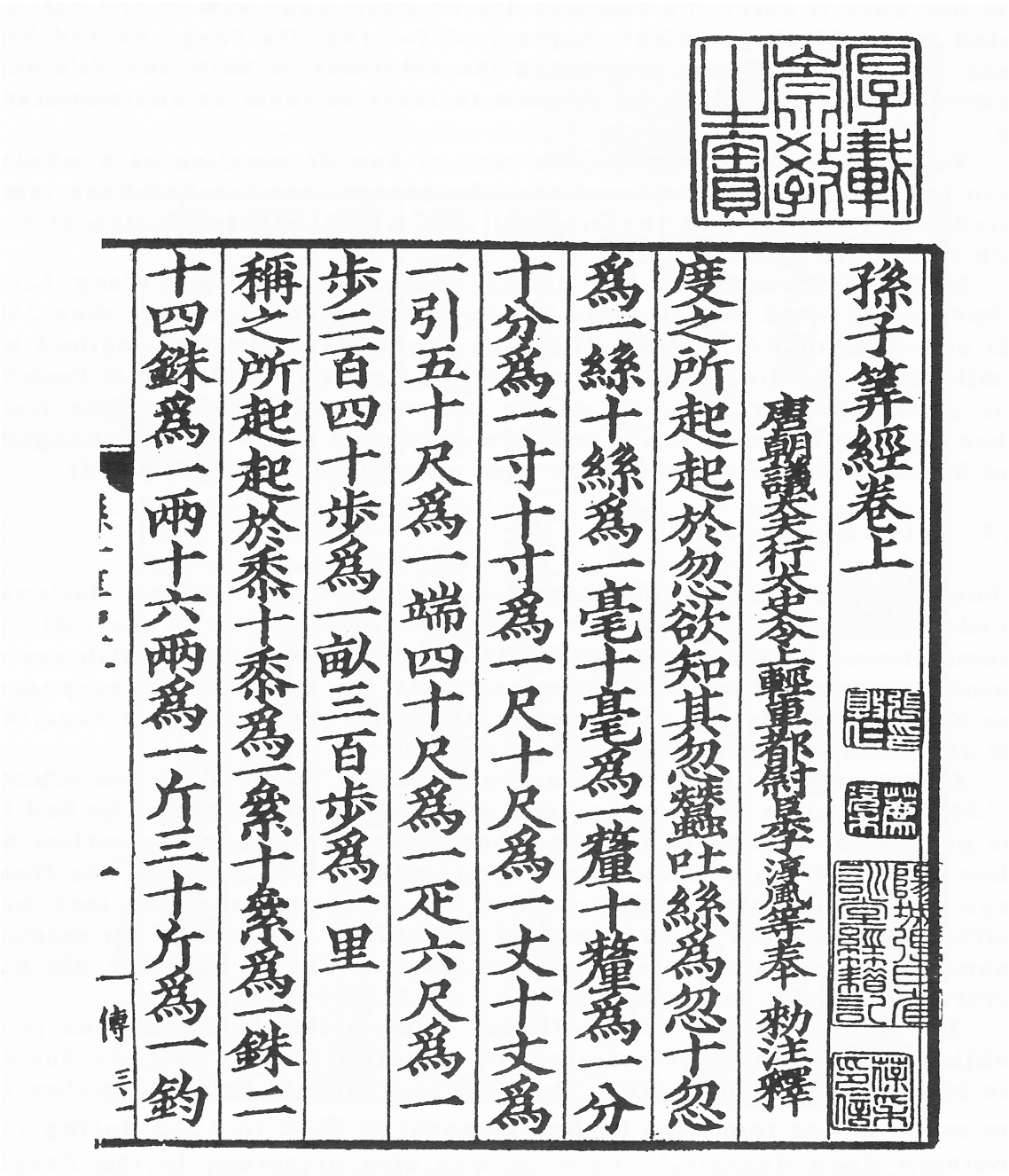
P. VOJTA (1991), "Siegel's theorem in the compact case". *Ann. of Math. (2)*, **133** (3), p. 509–548.

A. WEIL (1929), "L'arithmétique sur les courbes algébriques". *Acta Math.*, **52** (1), p. 281–315.

X. YUAN (2008), "Big line bundles on arithmetic varieties". *Invent. Math.*, **173**, p. 603–649. *arXiv:math.NT/0612424*.

S.-W. ZHANG (1995), "Positive line bundles on arithmetic varieties". *J. Amer. Math. Soc.*, **8**, p. 187–221.

S.-W. ZHANG (1998), "Equidistribution of small points on abelian varieties". *Ann. of Math.*, **147** (1), p. 159–165.


孫子算經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋

度之所起起於忽欲知其忽纖吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一釐十釐爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於黍十黍爲一絫十絫爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

FIGURE 1. The Sūnzǐ Suàngjīng (孫子算經, “The mathematical classic of Sūnzǐ”). — A print page from a Qing dynasty edition, reproduced from *Wikipedia*.

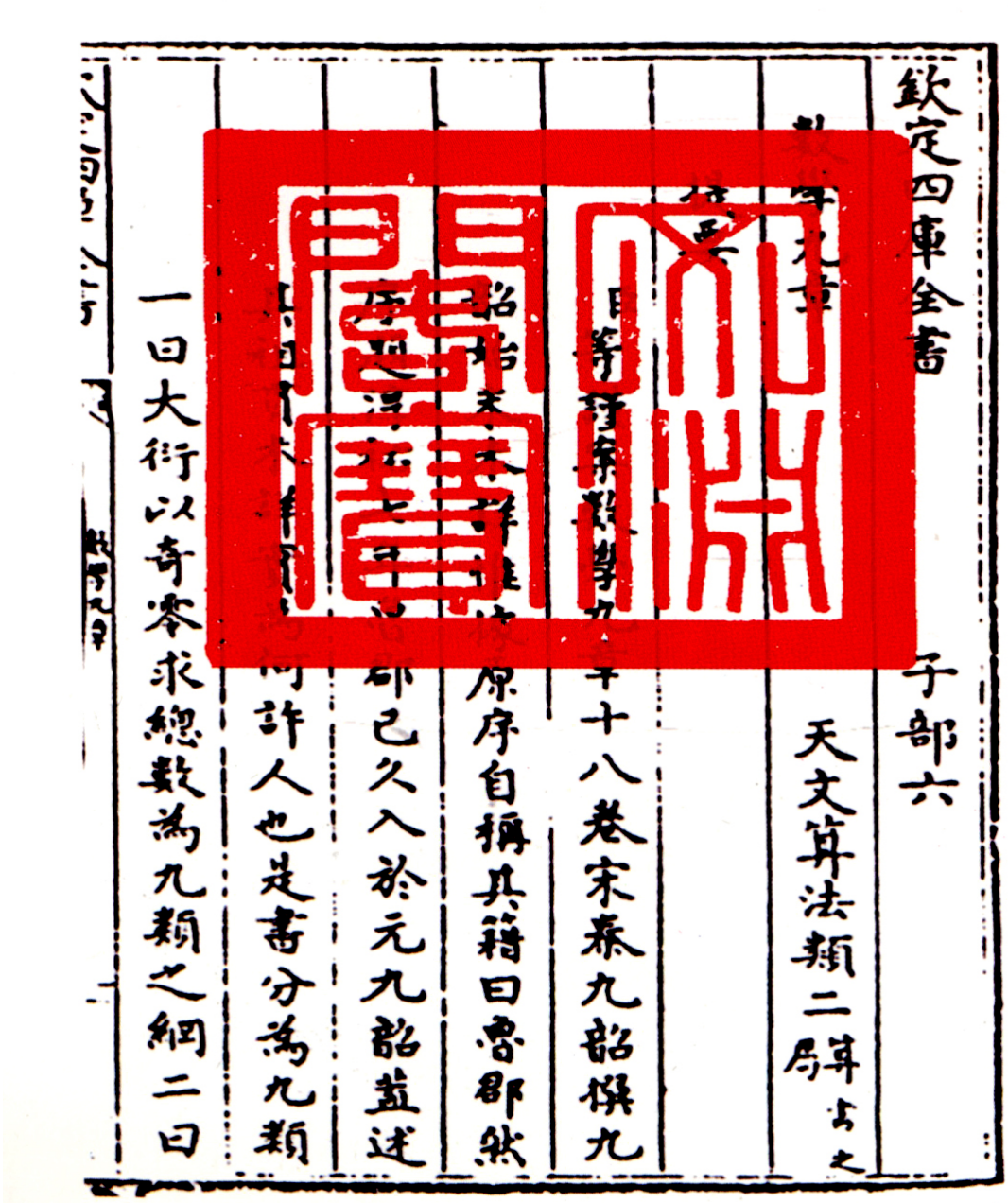


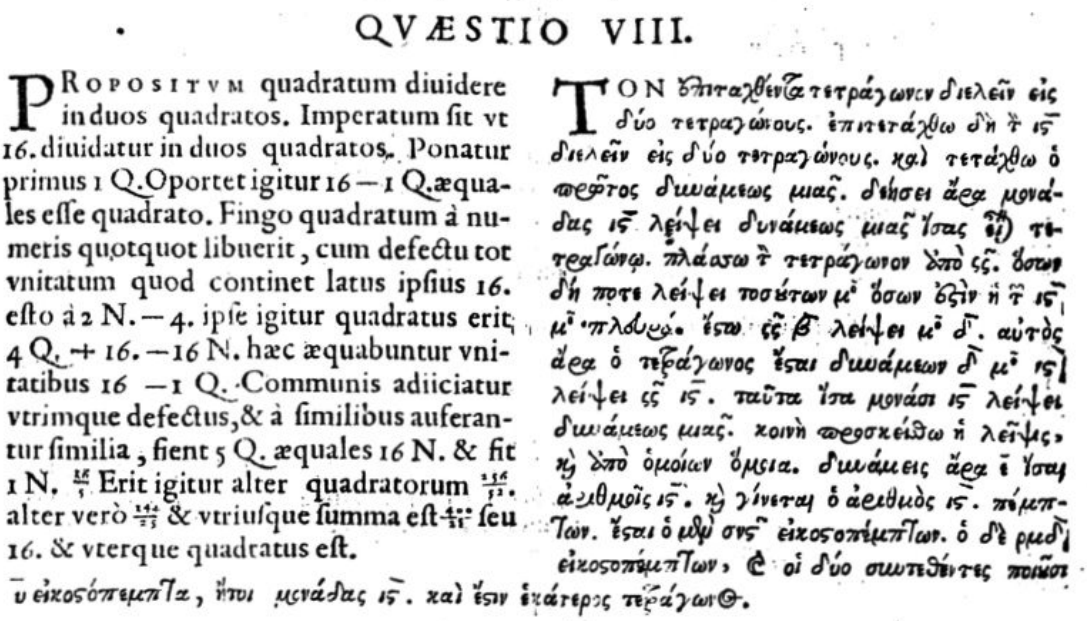
FIGURE 2. Mathematical Treatise in Nine Sections (數書九章, Shùshū Jiǔzhāng) from the 1847 Sìkù Quánshū 四庫全書. Reproduced from *Wikipedia*

Πρόβλημα,

ὅπερ Ἀρχιμήδης ἐν ἐπιγράμμασιν εὑρὼν τοῖς ἐν Ἀλεξανδρείᾳ περὶ ταῦτα πραγματευομένοις ζητεῖν ἐπέστειλεν ἐν τῇ πρὸς Ἐρατοσθένην τὸν Κυρηναῖον ἐπιστολῇ.

Πληθὺν Ἠελίοιο βοῶν, ὦ ξεῖνε, μέτρησον
φροντίδ' ἐπιστήσας, εἰ μετέχεις σοφίης,
πόσση ἄρ' ἐν πεδίοις Σικελῆς ποτ' ἐβόσκετο νήσου
Θρινακίης τετραχῇ στίφεα δασσαμένη
χροίην ἀλλάσσοντα· τὸ μὲν λευκοῖο γάλακτος,
κυανέῳ δ' ἕτερον χρώματι λαμπόμενον,
ἄλλο γε μὲν ξανθόν, τὸ δὲ ποικίλον. ἐν δὲ ἑκάστῳ
στίφει ἦσαν ταῦροι πλήθεσι βριθόμενοι
συμμετρίης τοιῆσδε τετευχότες· ἀργότριχας μέν
κυανέων ταύρων ἡμίσει ἠδὲ τρίτῳ
καὶ ξανθοῖς σύμπασιν ἴσους, ὦ ξεῖνε, νόησον,
αὐτὰρ κυανέους τῷ τετράτῳ τε μέρει
μικτοχρόων καὶ πέμπτῳ, ἔτι ξανθοῖσί τε πᾶσιν
τοὺς δ' ὑπολειπομένους ποικιλόχρωτας ἄθρει
ἀργεννῶν ταύρων ἕκτῳ μέρει ἑβδομάτῳ τε
καὶ ξανθοῖς αὖτις πᾶσιν ἰσαζομένους.
Θηλείαισι δὲ βουσὶ τάδ' ἔπλετο· λευκότριχες μέν
ἦσαν συμπάσης κυανέης ἀγέλης
τῷ τριτάτῳ τε μέρει καὶ τετράτῳ ἀτρεκὲς ἶσαι·
αὐτὰρ κυάνεαι τῷ τετράτῳ τε πάλιν
μικτοχρόων καὶ πέμπτῳ ὁμοῦ μέρει ἰσάζοντο
σὺν ταύροις· πάσης δ' εἰς νομὸν ἐρχομένης
ξανθοτρίχων ἀγέλης πέμπτῳ μέρει ἠδὲ καὶ ἕκτῳ
ποικίλαι ἰσάριθμον πλῆθος ἔχον τετραχῇ.
ξανθαὶ δ' ἠριθμεῦντο μέρους τρίτου ἡμίσει ἴσαι
ἀργεννῆς ἀγέλης ἑβδομάτῳ τε μέρει.
ξεῖνε, σὺ δ' Ἠελίοιο βοῶν πόσαι ἀτρεκὲς εἰπών,
χωρὶς μὲν ταύρων ζατρεφέων ἀριθμόν,
χωρὶς δ' αὖ θήλειαι ὅσαι κατὰ χρῶμα ἕκασται,
οὐκ ἄιδρίς κε λέγοι' οὐδ' ἀριθμῶν ἀδαής,
οὐ μὴν πώ γε σοφοῖς ἐναρίθμιος. ἀλλ' ἴθι φράζευ
καὶ τάδε πάντα βοῶν Ἠελίοιο πάθη.
ἀργότριχες ταῦροι μὲν ἐπεὶ μιξαίατο πληθύν
κυανέοις, ἵστανθ' ἔμπεδον ἰσόμετροι
εἰς βάθος εἰς εὐρός τε, τὰ δ' αὖ περιμήκεα πάντῃ
πίμπλαντο πλίνθου Θρινακίης πεδία.
ξανθοὶ δ' αὖτ' εἰς ἓν καὶ ποικίλοι ἀθροισθέντες
ἵστανθ' ἀμβολάδην ἐξ ἑνὸς ἀρχόμενοι
σχῆμα τελειοῦντες τὸ τρικράσπεδον οὔτε προσόντων
ἀλλοχρόων ταύρων οὔτ' ἐπιλειπομένων.
ταῦτα συνεξευρὼν καὶ ἐνὶ πραπίδεσσιν ἀθροίσας
καὶ πληθέων ἀποδοὺς, ὦ ξένε, πάντα μέτρα
ἔρχεο κυδιόων νικηφόρος, ἴσθι τε πάντως
κεκριμένος ταύτῃ ὄμπνιος ἐν σοφίῃ.

FIGURE 3. Archimedes's Cattle Problem, *Archimedis Opera omnia, cum commentariis Eutocii.* Edited by J. L. Heiberg, B. G. Teubner, Leibzig, Volume 2 (1881), pages 448–450



QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum ſit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 — 1 Q. æquales eſſe quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipſius 16. eſto à 2 N. — 4. ipſe igitur quadratus erit 4 Q. + 16. — 16 N. hæc æquabuntur vnitatibus 16 — 1 Q. Communis adiiciatur vtrimque defectus, & à ſimilibus auferantur ſimilia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriuſque ſumma eſt $\frac{400}{25}$ ſeu 16. & vterque quadratus eſt.

Τὸν δοθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτεταχθω δὴ τὸν ις διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις λεῖψει δυνάμεως μιᾶς ἴσας ἑξῆς τετραγώνῳ. πλάσω τὸ τετράγωνον ἀπὸ ς̄. ὅσων δὴ ποτε λείψει τοσούτων μ̄ ὅσων ὁ̄ς ἐστὶν ἡ τὸ ις μ̄ πλευρά. ἔστω ς̄ β̄ λείψει μ̄ δ̄. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ̄ μ̄ ις λείψει ς̄ ις̄. ταῦτα ἴσα μονάσι ις̄ λείψει δυνάμεως μιᾶς̄. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε̄ ἴσαι ἀριθμοῖς ις̄. καὶ γίνεται ὁ ἀριθμὸς ις̄. πέμπτων. ἔσται ὁ μὲν πρ̄ς̄ εἰκοσοπέμπτων. ὁ δὲ μεδ̄ εἰκοσοπέμπτων, ἃ οἱ δύο συντεθέντες ποιοῦσι ῡ εἰκοσόπεμπτα, ἥτοι μονάδας ις̄. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

FIGURE 4. Diophantus's *Arithmetica* with the comments of Fermat, stating his "Last Theorem" (1670 edition; reproduced from *Wikipedia*)