PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 23-33

Pietro Corvaja

A superficial viewpoint on certain Diophantine equations

Written by Abdelaziz El Habibi

Investigating solutions in integers of systems of algebraic equations is one of the main objects of Diophantine Geometry. Given polynomials $f_1(X_1, ..., X_N)$,...,$f_k(X_1, ..., X_N) \in \mathbb{Z}[X_1, ..., X_N]$, we consider the solutions $(x_1, ..., x_N) \in \mathbb{Z}^N$ or $\mathbb{Q}^N$ to the system

$$\begin{cases} f_1(x_1, ..., x_N) = 0 \\ \qquad \vdots \\ f_k(x_1, ..., x_N) = 0 \end{cases}$$

The complex solutions to the above system form an algebraic variety. We shall be especially interested in the case where such an algebraic variety is a surface. We shall see that many interesting open problems on Diophantine equations boil down to describing integral or rational points on algebraic surfaces; we shall then speak of *s*uperficial problems.

The Box problem and Euler bricks.

A first superficial problem about rational points is the so called the box problem: Does there exists a box whose sides, face diagonals and

space diagonal all have integral length ?
The equations corresponding to the box problem are the following:

$$\begin{cases} x_1^2 + x_2^2 = y_3^2 \\ x_2^2 + x_3^2 = y_1^2 \\ x_3^2 + x_1^2 = y_2^2 \\ x_1^2 + x_2^2 + x_3^2 = z^2 \end{cases} \tag{1}$$

Note that it is a system of homogenous equations. Viewing each solution as a point $(x_1 : x_2 : x_3 : y_1 : y_2 : y_3 : z)$ in the six-dimensional projective space, the system (1) defines an algebraic surface $\mathcal{S} \subset \mathbb{P}_6$. The points on this surface we are interested in are the rational points outside the 'trivial' curves where some coordinate vanishes.

The surface $\mathcal{S}$ is of general type: after Bombieri's Conjecture, it is believed that its rational points are not Zariski-dense. However, it is unkown whether it admits one single non-trivial rational point.

We could relax the conditions by omitting the requirement that the space diagonal of the box be rational. In other words, we are searching for triples of integers (x_1, x_2, x_3) such that any two of them belong to a Pytagorean triple. Such solids are common called Euler bricks. An example is given by the solution

$$(x_1 : x_2 : x_3 : y_1 : y_2 : y_3) = (44 : 117 : 240 : 267 : 244 : 125). \tag{2}$$

For this problem, the resulting surface is a (singular model of a) $K3$ surface; its rational points are Zariski-dense, as we shall now prove.

Let $\mathcal{X}$ be this surface, which is then defined in the five-dimensional projective space by the system of equations

$$\begin{cases} x_1^2 + x_2^2 = y_3^2 \\ x_2^2 + x_3^2 = y_1^2 \\ x_3^2 + x_1^2 = y_2^2 \end{cases} \tag{3}$$

First note that its only singularities are the isolated points

$$(0 : 0 : 1 : 1 : 1 : 0), (0 : 1 : 0 : 1 : 0 : 1), (1 : 0 : 0 : 0 : 1 : 1).$$

Letting C be the (plane) conic of equation $x_1^2 + x_2^2 = y_3^2$, the projection $\pi : \mathcal{X} \dashrightarrow C$ (undefined only on the first singular point) sending

$$\mathcal{X} \ni (x_1 : x_2 : x_3 : y_1 : y_2 : y_3) \mapsto (x_1 : x_2 : y_3)$$

admits for generic fibers the curves of genus 1 of equation

$$\begin{cases} x_2^2 + x_3^2 = y_1^2 \\ x_3^2 + x_1^2 = y_2^2 \end{cases} \tag{4}$$

These curves are irreducible and smooth whenever $x_1 x_2 y_3 \neq 0$. For each point $p = (x_1 : x_2 : y_3)$ on the conic C, the fiber $E_p = \pi^{-1}(p)$ admits a distinguished point O_p, namely the point

$$O_p = (x_1 : x_2 : 0 : x_2 : x_1 : y_3).$$

Taking the point O_p for the origin, a group law on E_p is well defined, so that E_p becomes an elliptic curve. Note the presence of three other rational points, namely $(x_1 : x_2 : 0 : -x_2 : x_1 : y_3), (x_1 : x_2 : 0 : x_2 : -x_1 : y_3)$ and $(x_1 : x_2 : 0 : -x_2 : -x_1 : y_3)$; these points are torsion points for the group law.

Consider now the following rational curve $\mathcal{D}$ on the surface, parametrized as follows: for every point $(a : b : c)$ in the conic $\mathcal{D}' : a^2 + b^2 = c^2$, put

$$\begin{cases} x_1 = a(4b^2 - c^2) \\ x_2 = b(4a^2 - c^2) \\ x_3 = 4abc \\ y_1 = b(4a^2 + c^2) \\ y_2 = a(4b^2 + c^2) \\ y_3 = c^3 \end{cases}$$

This curve, which gives rise to an infinite family of Euler bricks, was found by Saunders already in 1740.

Note that the map

$$(a : b : c) \mapsto \varphi(a : b : c) = (x_1 : x_2 : y_3)$$
$$= (a(4b^2 - c^2) : b(4a^2 - c^2) : c^3) \in C$$

is a degree three covering of the conic C by the isomorphic conic $\mathcal{D}'$ (which is also isomorphic to the rational curve $\mathcal{D} \subset \mathcal{X} \subset \mathbb{P}_5$). Now, each fiber E_p of the already described elliptic fibration intersects the conic in three points; if the point $p = (x_1 : x_2 : y_3) \in C$ comes from a rational point of $\mathcal{D}$ via the map φ described above, one of these points on E_p is rational. We then obtain that infinitely many elliptic curves E_p adimt an extra rational point, in addition to the point O_p and the three mentioned torsion points. This new rational point is in general of infinite order (as we shall see in a moment), so infinitely many fibers E_p contain infinitely many rational points. This shows that the rational points on the surface are Zariski-dense.

Geometrically, the points on E_p, coming from the curve $\mathcal{D}'$ can be described as follows: consider the two projections $\pi : \mathcal{X} \to C$ and $\varphi : \mathcal{D}' \to C$; the correponding fiber product gives rise to a new surface $\mathcal{Y}$ endowed with a finite map $\psi : \mathcal{Y} \to \mathcal{X}$ and an elliptic fibration $\mathcal{Y} \to \mathcal{D}'$. This elliptic fibration admits a section $\sigma : \mathcal{D} \to \mathcal{Y}$. The image of a point $q = (a : b : c) \in \mathcal{D}'$ is a point $\sigma(q) \in \mathcal{Y}$ such that

$$\pi(\psi(\sigma(q))) = \varphi(q).$$

It remains to show that infinitely many points $\sigma(q)$, for q a rational point on $\mathcal{D}'$ are non-torsion. By well-known result, this amounts to prove that σ is not identically torsion, which is equivalent to saying that for at least one point q, $\sigma(q)$ is non-torsion. We leave to the reader the task of verifying that for $q = (3 : 4 : 5)$ (the simples Pytagorean triple!), the image of $\sigma(q)$ on $\mathcal{X}$, namely the point appearing in (2), is non-torsion on the corresponding elliptic curve.

Let us come back to our original surface $\mathcal{S}$ whose (non-trivial) rational points correspond to the (possible) solutions to the original

Box problem. As we said, it is a surface of general type, and we do not know whether it contains any non-trivial rational point, and not even whether its rational points might form a infinite set, or a Zariski-dense set.

We conjecture the finiteness of its rational points, but we can prove unconditionally only the result below, for which we need the following definition: Let $\mathcal{R}$ be the radical function, associating to a positive real number the product of its prime divisors. Put

$$\mathcal{R}(x_1, x_2, x_3) := \mathcal{R}(\gcd(x_1, x_2).\gcd(x_2, x_3).\gcd(x_3, x_1)).$$

Then we can prove

Theorem 0.1 *For any (possible) infinite sequences in $\mathcal{S}(\mathbb{Q})$,*

$$\mathcal{R}(x_1, x_2, x_3) \longrightarrow \infty.$$

In the above statement, it is meant that the rational point $(x_1 : x_2 : x_3 : y_1 : y_2 : y_3 : z)$ is written with coprime integral coordinates. The Theorem impliess that one cannot take the coordinates to be *pairwise* coprime. Actually, it is easy to see that the prime 2 must divide at least one of the $\gcd(x_1, x_2)$, $\gcd(x_2, x_3)$, $\gcd(x_3, x_1)$; the theorem states moreover that infinitely many other primes must appear in the corresponding gcd, for every sequence of solutions.

Proof. The proof consists of an application of the Chevalley-Weil theorem; namely, we construct a finite covering $\mathcal{Z} \to \mathcal{X}$ to which the rational points of $\mathcal{X}$ can be lifted to points defined over a number field which only depends on $\mathcal{R}(x_1, x_2, x_3)$. Then apply Falting's theorem to the surface $\mathcal{Z}$, which turns out to be the product of two curves.

Suppose by contradiction that $\mathcal{R}(x_1, x_2, x_3)$ is bounded on an infinite sequence of rational points. Then there exists a finite set of primes S such that all the rational points in such a sequence never reduce to one singular point of the surface $\mathcal{S}$ modulo any prime outside the set S. In another language, they are S-integers with respect to the subvariety formed by the singular locus of the surface (note that after

desingularizing, such a locus becomes a finite union of irreducible curves).

For each pair of indices $1 \leq h < k \leq 3$, one of the equations (1) defining S implies that for each rational point of the surface the quantity $x_h^2 + x_k^2$ is a perfect square. Now, in the ring $\mathbb{Z}[i]$ the above expression factors as

$$x_h^2 + x_k^2 = (x_h + ix_k)(x_h - ix_k).$$

If the product is a square and the factors are coprime, each factor is a square (at least up to multiplication by a unit in the ring $\mathbb{Z}[i]$): this is the basic principle behind the so called Chevalley-Weil theorem. We are supposing that the two factors can have common prime divisors only outside the set S (more precisely, outside the set of primes in $Z[i]$ lying above one prime of S). Hence, there exists a finite extension κ of $\mathbb{Q}(i)$ such that each factor $x_h + ix_k$ is a square in the ring of integers of such a number field.

We then obtain that the rational points on $\mathcal{S}$ lift to κ- rational points on the variety defined by the system of equations

$$\begin{cases} x_1 + ix_2 = u_3^2 \\ x_1 - ix_2 = v_3^2 \\ x_2 + ix_3 = u_1^2 \\ x_2 - ix_3 = v_1^2 \\ x_3 + ix_1 = u_2^2 \\ x_3 - ix_1 = v_2^2 \\ x_1^2 + x_2^2 + x_3^2 = z^2 \end{cases} \tag{5}$$

This is the equation of another surface $\mathcal{Z}$ covering by a finite map (of degree 8) our surface $\mathcal{S}$. We claim that Z is isomorphic to the product of a genus 5 curve with itself. Then, by Faltings' theorem, the surface $\mathcal{Z}$ contains only finitely many rational point on any given number field, concluding the argument.

Let us prove our claim. Looking first at the last equation in (5), we see that the surface $\mathcal{Z}$ is a degree 64 cover of a smooth quadric,

which is isomorphic, over the complex (and even over the number field $\mathbb{Q}(i)$) to the square of the projective line. The covering $\mathcal{Z} \to \mathbb{P}_1 \times \mathbb{P}_1$ ramifies only over the curves of equation $x_h \pm i x_h = 0$, which are pairs of lines. Removing their pre-images from the surface $\mathcal{Z}$, and calling $\mathcal{Z}^*$ the corresponding open surface, we obtain an unramified cover $\mathcal{Z}^* \to (\mathbb{P}_1 \setminus (F))^2$, where F is a finite set of cardinality 6. Now, every unramified covering of a product is covered by a product of unramified covers; in our case, we have an abelian unramified cover of $\mathbb{P}_1 \setminus F$, of type $(2, 2, 2)$, obtained as a fibred product of three degree 2 covers each ramified over two points; the genus of the resulting curve turns out to be five, so Faltings' theorem provides finiteness.

The Markov equation

The equation

$$x^2 + y^2 + z^2 = 3xyz,$$

is called the Markov equation. It is the equation of a singular affine surface $\mathcal{M}$ in three-space. Markov triples are defined as the solutions (x, y, z), with x, y, z positive integers, to Markov's equation; we call any positive integer x which appears in a Markov triple a Markov number, and we call any pair (x, y) such that for some integer z the triple (x, y, z) is a Markov triple a *Markov pair*. A question about the arithmetic nature of Markov numbers is the following: does the greatest prime factor of a Markov number tend to infinity? If not, there would exist infinitely many Markov numbers which are S-units for a fixed finite set of places S; it is still an open problem.

Recalling that $\mathcal{R}(.)$ denotes the radical of an integer the problem boils down to understanding whther $\mathcal{R}(x)$ must tend to infinity on every infinite sequence of Markov numbers. We do not know the answer, but dispose of the weaker result:

Theorem 0.2 (Theorem 1 in [2]) *For every infinite sequences of Markov pairs, we have*

$$\mathcal{R}(xy) \longrightarrow \infty.$$

Idea of the proof. The proof uses the subspace theorem after reducing to a problem about itegral points. Suppose that $\mathcal{R}(xy)$ is bounded on an infinite sequence. Then for some fixed integer R, the Markov equation has infinitely many solutions (x, y, z) where $z \in \mathbb{Z}$ and x, y are units in the ring $\mathbb{Z}[1/R]$.

Note that once x, y are fixed integers, the Markov equation in z can be solved whenever the quantity

$$9x^2y^2 - 4(x^2 + y^2)$$

is a perfect square. Putting $x^2 = u, y^2 = v$ we obtain the quadratic equation

$$9uv - 4u - 4v = \delta^2,$$

which in homogeneous form becomes

$$9uv - 4uw - 4vw = \delta^2. \tag{6}$$

This is the equation of a smooth quadric surface in $\mathbb{P}_3$. The condition that u, v, δ are integers amounts to an integrality condition on the rational point $(u : v : w : \delta)$ with respect to the divisor $w = 0$ on the surface (see [1], chap. 1 for a precise definition of the notion of integrality with respect to a divisor). Similarly, requiring that x, y, so u, v, are R-units amounts to the integrality with respect to the divisor $uv = 0$. We must then consider the complement of the divisor D of equation $uvw = 0$ on the smooth quadric defined by (6). This divisor is the sum of three smooth conics; identifying the surface with the product $\mathbb{P}_1 \times \mathbb{P}_1$, the divisor D has bidegree $(3, 3)$; note that any canonical divisor K on $\mathbb{P}_1 \times \mathbb{P}_1$ had bidegree $(-2 - 2)$, so the sum $D + K$ is ample. According to Vojta's Conjecture, the D-integral points on the surface should not be Zariski-dense. Although we are not able to prove Vojta's Conjecture for this class of open surfaces, an application of the Subspace Theorem as described in [2] proves the desired result when z is supposed to be an integer in the classical sense, not merely an R-integer.

Elliptic curves over $\mathbb{Q}$

Let E be an elliptic curve over $\mathbb{Q}$ be defined by a Weierstrass equation:

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

where $a, b \in \mathbb{Z}$ are integers with $4a^3 - 27b^2 \neq 0$. For a rational solution $P = (x_1, x_2) \in \mathbb{Q}^2$ of the above equation, one can write the rational numbers x, y in a unique way as

$$(x, y) = (\tfrac{u}{d^2}, \tfrac{v}{d^3}),$$

for coprime integers u, v and $d > 0$. We define the denominator of $P = (x, y)$ to be the integer $d(P) = d$.

The following Conjecture, which is a consequence of Vojta's conjecture on surfaces, gives a criterion for identifying elliptic curves by studying the denominators of their rational points.

Conjecture 1 *Let E_1 and E_2 be two elliptic curves over $\mathbb{Q}$ with infinitely many rational points. Suppose there exist infinitely many pairs $(P_1, P_2) \in E_1(\mathbb{Q}) \times E_2(\mathbb{Q})$ for which*

$$(*) \quad d(P_1) = d(P_2).$$

Then E_1 and E_2 are isomorphic, and after identifying $E_1 \simeq E_2$, for all but finitely many solutions (P_1, P_2) to $(*)$, $P_1 = \pm P_2$.

Although the problem is formulated in terms of rational points on curves, it turns out to be in fact a problem on integral points on surfaces, as we shall see in a moment. We first recall a related result of Corrles-Rodriganez and Schoof from [4]:

Proposition 0.3 *Let $P_1 \in E_1(\mathbb{Q})$ and $P_2 \in E_2(\mathbb{Q})$ of infinite order; if*

$$\mathcal{R}(d(nP_1))|\mathcal{R}(d(nP_2))$$

for all $n \in \mathbb{N}$, then E_1 and E_2 are isogenous over $\mathbb{Q}$.

A second conclusion asserts that for all but finitely many solutions, P_2 is the image of P_1 by a suitable isogeny $E_1 \to E_2$.

The next theorem is a particular case of the above Conjecture; it is a curious application of a general result of Vojta on subvarieties of semi-abelian varieties.

Theorem 0.4 *Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$. Suppose that for infinitely many pairs $(P_1, P_2) \in E_1(\mathbb{Q}) \times E_2(\mathbb{Q})$,*

$$d(P_1) = d(P_2) \quad \text{and} \quad d(2P_1) = d(2P_2). \tag{7}$$

Then E_1 is isomorphic to E_2 and, after identifying E_1 with E_2, for all but finitely many such pairs, $P_1 = \pm P_2$.

This is Theorem 3.32 in [3]. The proof consists in viewing the solutions to (7) as integral points on the complement of a certain divisors in a blow-up of the surface $E_1 \times E_2$. Such an open surface can be embedded into a semi-abelian variety, namely the product of the multiplicative group by the abelian surface $E - 1 \times E_2$, and then the mentioned result by Vojta applies.

References

[1] P. Corvaja, *Integral Points on Algebraic Varieties. An introduction to Diophantine Geometry. Institute of Mathematical Sciences Lecture Notes, Hindustan Book Agency, New Delhi*, 2016.

[2] P. Corvaja and U. Zannier *On the greatest prime factor of Markov pairs*, *Rendiconti del Seminario Mat. della Università di Padova*, 116:253–260, 2006.

[3] P. Corvaja and U. Zannier *Applications of Diophantine Approximation to Integral Points and Transcendence*, *Cambridge Tracts in Mathematics* 212, Cambridge University Press, 2018.

[4] C. Corrales and R. Schoof *The support problem and its elliptic analogue*, *J. Number Theory*, 64:276–290, 1997.

[5] J.H. Silverman, J. Tate, *Rational points on elliptic curves*, *Second edition, Springer*, 2015.

Abdelaziz EL Habibi
Department of Mathematics and Informatics
Mohammed First University
BV Mohammed VI BP 717 60000 Oujda, Morocco.
email: abdelaziz.elhabibi92@gmail.com