Revue d'histoire des mathématiques,
8 (2002), p. 67–111.

SOLVING AN INDETERMINATE THIRD DEGREE EQUATION IN RATIONAL NUMBERS. SYLVESTER AND LUCAS

Tatiana Lavrinenko (*)

Abstract. — This article concerns the problem of solving Diophantine equations in rational numbers. It traces the way in which the 19th century broke from the centuries-old tradition of the purely algebraic treatment of this problem. Special attention is paid to Sylvester's work "On Certain Ternary Cubic-Form Equations" (1879–1880), in which the algebraico-geometrical approach was applied to the study of an indeterminate equation of third degree.

Résumé. — Résolution en nombres rationnels des équations indéterminées du 3e degré: Sylvester et Lucas. — L'article est consacré au problème de la résolution des équations diophantiennes en nombres rationnels. On examine comment s'est passée, au XIXe siècle, la transition d'un traitement purement algébrique caractéristique des travaux de Diophante à Cauchy, vers des recherches en termes de géométrie algébrique. L'article analyse notamment l'écrit de Sylvester "*On Certain Ternary Cubic-Form Equations*" (1879–1880), où l'approche de géométrie algébrique était utilisée pour étudier les équations indéterminées du 3e degré.

1. INTRODUCTION

As is well-known, Poincaré laid the foundation for the arithmetic of algebraic curves in his study of the structure of the rational points set of such curves, namely his paper "*Sur les propriétés arithmétiques des courbes algébriques*" [Poincaré 1901]. His work can be interpreted as

(*) Texte reçu le 26 mars 2001, révisé le 14 mars 2002.
Tatiana Lavrinenko, Department of Mathematics, Moscow State University of Commerce, Smol'naya 36, Moscow 125817 (Russia).
Courrier électronique: belalavt@mtu-net.ru
I would like to give my special thanks to the two anonymous referees, whose remarks were extremely helpful in my work on the paper.

Keywords: Diophantine equations, algebraic geometry, elliptic curve, rational point, Lucas, Sylvester, Story.

AMS classification: 01A55, 11G05, 14G05, 14H52.

the study of the set of rational solutions of either an indeterminate, or Diophantine, equation

$$f(x, y) = 0 \tag{1}$$

where $f(x, y)$ is a polynomial in two variables x, y with rational coefficients, or an indeterminate equation

$$F(u, v, w) = 0 \tag{2}$$

where $F(u, v, w)$ is a homogeneous polynomial in the variables u, v, w with rational coefficients. Indeed, we can interpret (1) as an equation of some curve in Cartesian coordinates x, y and (2) as an equation of a plane curve in homogeneous coordinates u, v, w. Without loss of generality, the coefficients in (2) can be considered integer, and because of homogeneity, the problem of solving equation (2) over the rational numbers is equivalent to the problem of its solution over the integers.

As a basis for classifying indeterminate equations, Poincaré took the concept of birational equivalence (over the field $\mathbb{Q}$ of rational numbers).[1] His investigation showed that the most important properties of the set of rational solutions of equation (2) are determined by the corresponding curve's genus, which is a birational invariant, and not by the degree of this polynomial. In [Poincaré 1901], the main results dealing with the set of rational points of curves of genus 0 were proved (they had also been obtained by Gilbert and Hurwitz 10 years before), and the principles for the study of the arithmetic of curves of genus 1 (that is elliptic curves) were founded. Poincaré established that an elliptic curve, which has a rational point, is birationally equivalent to some curve of third degree. Thus, in this case, the problem reduces to the investigation of curves of the third degree. For them, Poincaré considers two procedures: a) determination of a new rational point of the curve from a known rational point P as the point of intersection of the curve with the tangent line to the curve at P (the

[1] Recall that in Diophantine analysis two absolutely irreducible algebraic curves X and Y, given by equations with coefficients from the field $\mathbb{Q}$, are termed birationally equivalent, or birationally isomorphic, if there exist $\mathbb{Q}$-rational maps (*i.e.*, maps given by rational functions with coefficients from the field $\mathbb{Q}$) from X to Y and from Y to X, which are inverse to each other. Poincaré [1901] calls such maps "*transformations birationnelles à coefficients rationnels*".

tangent method); b) determination of a new rational point of the curve from two known rational points M and N as the third point of the curve's intersection with the straight line drawn through M and N (the secant method). To describe the set of rational points, which can be obtained by means of these procedures, Poincaré uses a parametric representation of a cubic curve by means of elliptic functions. He shows that the rational point with an elliptic argument α generates on a cubic curve a set of rational points with elliptic arguments $(3k+1)\alpha$, $k \in \mathbb{Z}$, by means of the tangent and secant methods. Proceeding from several rational points of a cubic with elliptic arguments $\alpha, \alpha_1, \ldots, \alpha_q$, one can obtain rational points with elliptic arguments

$$\alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \cdots + p_q(\alpha_q - \alpha), \tag{3}$$

where $n, p_i \in \mathbb{Z}$, by means of the tangent and secant methods.[2] Poincaré writes: "*On peut se proposer de choisir les arguments* $\alpha, \alpha_1, \ldots, \alpha_q$, *de telle façon que la formule* (3) *comprenne tous les points rationnels de la cubique*" [Poincaré 1901, p. 492*f*]. He calls the least number $q+1$ of rational points of a cubic possessing such a quality, the rank of a cubic. Poincaré poses the question: "*Quelles valeurs peut-on attribuer au nombre entier que nous avons appelé le rang d'une cubique rationnelle?*" [Poincaré 1901, p. 492*f*]. In the definition of the rank and in the question as posed, mathematicians recognized a tacit supposition about the finiteness of the rank. This supposition, subsequently called Poincaré's hypothesis, was proved by Mordell in 1922. After Poincaré's investigation, there remained one more step to take in order to get a clear description of the structure of the set of rational points on a cubic curve of genus 1: to introduce the operation of adding rational points by means of the tangent and secant methods in such a way that the addition of points corresponded to the addition of their elliptic arguments. This step, according to Schappacher [1991, p. 179], was taken by the middle of the 1920s. It is not difficult to establish that the set of rational points of a cubic forms an abelian group with respect to the introduced operation. Poincaré's hypothesis, proved by Mordell, implies that this group is finitely generated.

[2] The expression (3) can be presented in a more symmetrical form, as $m\alpha + m_1\alpha_1 + \cdots + m_q\alpha_q$, where $m, m_1, \ldots, m_q \in \mathbb{Z}$ and $m + m_1 + \cdots + m_q \equiv 1 \pmod 3$. And if we add a point with elliptic argument 0 to the initial system of rational points with elliptic arguments $\alpha, \alpha_1, \ldots, \alpha_q$, then $m, m_1, \ldots, m_q$ can assume any integer values.

Poincaré's work can be considered as the beginning of a new stage in the investigation of indeterminate equations characterized by a new algebraico-geometrical view of the problem and by the use of concepts and results from the theory of algebraic curves. The earlier period in the study of indeterminate equations (at least up to the 1870s) was based entirely upon an algebraic approach to their solution. It had long seemed that the algebraic methods of Diophantus, Fermat, and Euler had nothing in common with the modern methods of finding rational points on algebraic curves and that these algebraic methods had completely exhausted themselves in the solution of separate indeterminate equations and of a small number of types already in Euler's works. However from the 1960s on, a new interpretative model was built mostly by Russian historians, who brought a new reading to the fore. In this new view suggested and substantiated in [Hofmann 1961], [Bashmakova 1968 and 1981], [Kauchikas 1979], [Weil 1983], [Lavrinenko 1983], [Rashed 1984] for example, the ancient algebraic methods of solving indeterminate equations may be interpreted geometrically, and even, according to some investigations, in terms of the modern algebraico-geometrical approach. The presence, in the works of Fermat and Euler, of general methods still used today in the arithmetic of elliptic curves is likewise noted by [Ellison 1978]. Indeed, using a purely algebraic approach to indeterminate equations, methods were obtained of determining new rational solutions from one or two known rational solutions of third degree equations of the following kind

$$y^2 = f_3(x) \quad \text{or} \quad y^3 = f_3(x), \tag{4}$$

where $f_3(x)$ is a polynomial of third degree with rational coefficients. Simple geometrical interpretation of these methods gives just the tangent and secant methods (see [Bashmakova 1981], [Lavrinenko 1988]; for the geometrical interpretation of Fermat's methods in the literature on the history of mathematics as well as for a detailed bibliography, see [Goldstein 1995]). Still, neither Euler's works nor those of Fermat and Diophantus contain any such geometrical interpretations. That is why the question of historical interpretation is important here. Various positions were expressed by different researchers, but this will not be our issue here. We will leave this question out. The greatest achievements of the algebraic

approach in the arithmetic of elliptic curves were, first of all, Lagrange's formulation of the method for finding a new rational solution from one known rational solution of the general equation of third degree

$$(5)\quad f_3(x,y) \equiv a+bx+cy+dx^2+exy+fy^2+gx^3+hx^2y+kxy^2+\ell y^3 = 0$$

with rational coefficients [Lagrange 1777] and, secondly, methods stated by Cauchy [1826] in his work "*Sur la résolution de quelques équations indéterminées en nombres entiers*" for finding a new solution in integers from one or two known solutions in integers of the general homogeneous equation of third degree

$$(6)\quad F(x,y,z) \equiv Ax^3+By^3+Cz^3+Dyz^2+Ezx^2 + Fxy^2+Gzy^2+Hxz^2+Iyx^2+Kxyz = 0$$

with integer coefficients. These methods also admit simple geometrical interpretation and present nothing but the tangent and secant methods for third degree equations of the most general form, the latter formulated, however, not in terms of geometry but purely analytically. And, although works appeared throughout the nineteenth century which considered Diophantine equations purely algebraically, no further general results in the arithmetic of elliptic curves were obtained in this way.

The question this paper wants to address is the following: How did the transition take place from the traditional algebraic approach to solving indeterminate third degree equations in rational numbers to the new approach stated in Poincaré's work? Did Poincaré have any predecessors?[3] The present study, without being comprehensive, focusses on some 19th-century investigations reflective of this transition. Special attention will be paid to Sylvester's work "On Certain Ternary Cubic-Form Equations" [Sylvester 1879/1880].

Two steps were necessary to have the transition take place:

[3] Note that Poincaré's first predecessor in applying an analytical approach to Diophantine equations was Jacobi. He pointed out the possibility of using theorems concerning the addition of elliptic integrals for studying the set of rational solutions of Diophantine equations of the type (4) with $y^2 = f_3(x)$ in his work [Jacobi 1835] (see [Schlesinger 1909], [Bashmakova 1981]). Apparently, this idea did not attract the attention of mathematicians in the 19th century. We don't find any attempts to apply the theory of elliptic integrals and functions to the study of Diophantine equations in the works of that time (at least up to 1880).