

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 3^e 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 XIX^e 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 3^e 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

$$(1) \quad f(x, y) = 0$$

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

$$(2) \quad F(u, v, w) = 0$$

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 $\alpha, \alpha_1, \dots, \alpha_q$, one can obtain rational points with elliptic arguments

$$(3) \quad \alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \dots + p_q(\alpha_q - \alpha),$$

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 $\alpha, \alpha_1, \dots, \alpha_q$, de telle façon que la formule (3) comprenne tous les points rationnels de la cubique*” [Poincaré 1901, p. 492f]. 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. 492f]. 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 $m\alpha + m_1\alpha_1 + \dots + m_q\alpha_q$, where $m, m_1, \dots, m_q \in \mathbb{Z}$ and $m + m_1 + \dots + m_q \equiv 1 \pmod{3}$. And if we add a point with elliptic argument 0 to the initial system of rational points with elliptic arguments $\alpha, \alpha_1, \dots, \alpha_q$, then m, m_1, \dots, 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

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

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).

First, to formulate geometrically the problem of solving the third degree Diophantine equations, and its solving methods, by means of the tangent and the secant.

Second, to pass from the problem of finding separate rational solutions for such equations to the consideration and investigation of the whole set of rational solutions and its structure.

These two steps will be considered in detail in the following two sections. A last section is devoted to the study of William Story's reformulation using elliptic functions, and his extension of Sylvester's theory.

2. GEOMETRICAL INTERPRETATION OF SOLVING THIRD DEGREE DIOPHANTINE EQUATIONS AND OF THE TANGENT AND SECANT METHODS: NEWTON, LUCAS, SYLVESTER

Newton's papers reveal Newton's command of the secant method in its geometrical formulation (see [Bashmakova 1981]; [Schappacher 1991]). However, Newton's considerations became known only after the publication of his papers in 1971 [Newton 1971]. The tangent and secant methods for a general third degree equation, setting the plane cubic curve, were originally introduced into mathematics purely algebraically, that is, without any appeal to geometrical notions; Lagrange introduced the tangent method in 1777, whereas Cauchy treated the tangent and secant methods in 1826.⁴

Note that Cauchy considered the homogeneous equation (6) and that for a geometrical interpretation of his methods, it was necessary to treat equation (6) as an equation of a plane curve in homogeneous projective coordinates. These coordinates, however, were introduced only several years after the publication of [Cauchy 1826].

In 1878, when a developed theory of algebraic curves considered on the projective plane already existed, the French mathematician Edouard Lucas published an article which formulated the problem of solving an indeterminate third degree equation and the tangent and secant methods

⁴ Both Lagrange and Cauchy use partial derivatives of polynomials of third degree in transformations of these polynomials. This, by the way, helps in appreciating the geometrical meaning of Lagrange's and Cauchy's algebraic methods, equivalent to the tangent method. For a detailed consideration of their methods, see [Lavrinenko 1985].

geometrically [Lucas 1878]. These formulations sound quite up-to-date: “*Considérons l’équation du troisième degré*

$$(I) \quad f(x, y, z) = 0$$

d’une courbe en coordonnées rectilignes et homogènes; soit m_1 un point dont les coordonnées (x_1, y_1, z_1) sont rationnelles, et qu’il est facile de rendre entières; on a ainsi une première solution en nombres entiers de l’équation proposée. On peut obtenir de nouvelles solutions, en nombres entiers, de l’équation, par l’un des trois procédés suivants:

1) *Si l’on mène la tangente à la courbe en m_1 , cette droite rencontre la courbe en un autre point m dont les coordonnées sont encore rationnelles; par conséquent, d’une première solution de l’équation (I) on déduit, en général, une nouvelle solution (x, y, z) de cette équation, par les formules*

$$f(x, y, z) = 0, \quad x \frac{df}{dx_1} + y \frac{df}{dy_1} + z \frac{df}{dz_1} = 0.$$

Cependant, lorsque la tangente est parallèle à l’une des asymptotes, ou lorsque la tangente est menée par un point d’inflexion, on n’obtient pas de solutions nouvelles.

2) *Si m_1 et m_2 désignent deux points dont les coordonnées (x_1, y_1, z_1) et (x_2, y_2, z_2) sont rationnelles, et par conséquent entières, on obtient, en général, une nouvelle solution, en prenant l’intersection de la sécante m_1m_2 avec la courbe, c’est-à-dire par les équations*

$$f(x, y, z) = 0, \quad \begin{vmatrix} x & y & z \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = 0,$$

en tenant compte des relations

$$f(x_1, y_1, z_1) = 0, \quad f(x_2, y_2, z_2) = 0”$$

[Lucas 1878, pp. 507–508]. The third procedure considered by Lucas consists of finding the sixth point of intersection of the cubic curve with the conic drawn through five known rational points of the cubic curve. The introduction of geometrical language into Diophantine analysis was an important factor in the history of this discipline, since it paved the way for the introduction of ideas from algebraic geometry. This thus connected

Diophantine analysis with ideas from a developed mathematical theory, whereas it had previously been confined to elementary considerations of an algebraic character. Great merits belong to Lucas in taking this important step.

In his work, Lucas repeatedly mentioned [Cauchy 1826]. So, in 1873, Lucas published his extensive *Recherches sur l'analyse indéterminée et l'arithmétique de Diophante* [Lucas 1873], a work devoted primarily to the investigation of equations of the form $Ax^4 + By^4 = Cz^2$ using the method of infinite descent.⁵ In this same work, Lucas gives information of an historical character about the development of Diophantine analysis and also states some of the known methods for finding rational solutions to indeterminate third and fourth degree equations.⁶ With reference to [Cauchy 1826], he gives the following formulae for finding a new rational solution to the equation

$$(7) \quad AX^3 + BY^3 + CZ^3 + 3DXYZ = 0$$

from two known rational solutions (x, y, z) and (x_1, y_1, z_1) :

$$(8) \quad \begin{cases} X = Byy_1(xy_1 - x_1y) + Czz_1(xz_1 - x_1z) + D(x^2y_1z_1 - x_1^2yz), \\ Y = Czz_1(yz_1 - y_1z) + Axx_1(yx_1 - y_1x) + D(y^2z_1x_1 - y_1^2zx), \\ Z = Axx_1(zx_1 - z_1x) + Byy_1(z_1y - zy_1) + D(z^2x_1y_1 - z_1^2xy). \end{cases}$$

Indeed, in [Cauchy 1826], after the deduction of formulae corresponding to the secant method for the general equation (6), a particular case of the equation (7) is considered, and the formulae (8) are deduced. Apparently, under the influence of [Cauchy 1826], though without mentioning it, Lucas

⁵ The problem of solving the equation $Ax^4 + By^4 = Cz^2$ in integers corresponds to the problem of solving the equation $Au^4 + B = Cv^2$ in rational numbers. Lucas uses the idea of infinite descent not so much for the proof of the insolubility of indeterminate equations, as for obtaining procedures for finding successively all integer solutions of an indeterminate equation from its "least" integer solution. On the level of the ideas, Lucas's investigations are close to those of Lagrange on the indeterminate equations $2x^4 - y^4 = \pm z^2$ and $x^4 + 8y^4 = z^2$ [Lagrange 1777].

⁶ These are Lagrange's method for finding a new rational solution of the equation (5) from a known rational solution (given by Lucas without any reference to Lagrange) and methods of finding rational solutions of the equation $f_4(x) = y^2$, where $f_4(x)$ is a polynomial of fourth degree with rational coefficients, by means of quadratic substitutions (they are given with reference to Fermat).

formulated the following statements, which he considered in the 1875 issue of the *Nouvelles annales de mathématiques*:

“1) Si (x, y, z) représente une solution en nombres entiers de l'équation indéterminée

$$Ax^3 + By^3 + Cz^3 + 3Dxyz = 0,$$

on obtient une nouvelle solution à l'aide des équations

$$(9) \quad \frac{X}{x} + \frac{Y}{y} + \frac{Z}{z} = 0,$$

$$(10) \quad AXx^2 + BYy^2 + CZz^2 = 0.$$

2) Si (x, y, z) et (x_1, y_1, z_1) désignent deux solutions distinctes de l'équation précédente, on obtient une nouvelle solution à l'aide des équations

$$(11) \quad \begin{vmatrix} X & Y & Z \\ x & y & z \\ x_1 & y_1 & z_1 \end{vmatrix} = 0,$$

$$(12) \quad AXxx_1 + BYyy_1 + CZzz_1 = 0''$$

[Lucas 1875]. One can check that the solution (X, Y, Z) of the system (9)–(10), which is considered in Lucas's first statement, coincides with the solution of the equation (7), obtained by means of the tangent method from its known solution (x, y, z) . Essentially, this was shown in [Cauchy 1826]. Indeed, Cauchy, having first stated the algebraic equivalent of the tangent method for the equation (6), applies it to the equation $AX^3 + BY^3 + CZ^3 = 0$. He shows that in this case the new solution (X, Y, Z) obtained from the known solution (x, y, z) will satisfy not only (10) but also (9) (stating Cauchy's results we use, here and further on, Lucas's designations). Solving the system (9)–(10), Cauchy obtains formulae for the new solution:

$$(13) \quad X = x(By^3 - Cz^3), \quad Y = y(Cz^3 - Ax^3), \quad Z = z(Ax^3 - By^3).$$

Further, considering the tangent method (in an algebraic form!), as applied to (7), Cauchy shows that in this case a new rational solution is also found according to the formulae (13). Consequently, the new

solution of (7) can also be found by solving (9)–(10). But this is just Lucas’s first statement. The solution (X, Y, Z) of (7), considered in Lucas’s second statement, in fact coincides with the solution obtained from the known solutions (x, y, z) and (x_1, y_1, z_1) by means of the secant method. Algebraically, it may be shown in this way. In [Cauchy 1826], the solution determined by the secant method appears as

$$(14) \quad X = xs - x_1t, \quad Y = ys - y_1t, \quad Z = zs - z_1t,$$

where parameters s and t are determined as a result of substituting expressions for X, Y , and Z into (6). In the same way, Cauchy also obtains formulae (8) for (7), which were given in [Lucas 1873]. It is obvious that if X, Y, Z are set by the formulae (14), then (11) will be true. On the other hand, a simple check shows that X, Y, Z determined by the formulae (8) satisfy (12) as well. Therefore, solving the system (11)–(12), we obtain the solution (X, Y, Z) of the equation (7) determined by the formulae (8). This is precisely the solution found by means of Cauchy’s second method or the secant method. Unlike relations (9) and (10), relations (11) and (12) are not to be found in [Cauchy 1826], *i.e.*, this way of stating the results is apparently Lucas’s own. The two statements concerning integral solutions of (7) are again stated in [Lucas 1877], now with reference to [Cauchy 1826]. Lucas writes that the results obtained by Cauchy for (7) can be given in the form Lucas considers new [Lucas 1877, Chap. II, § 2]. Further, he cites statements from [Lucas 1875], which were considered above.

It is easy to see that the form of the second procedure, given in [Lucas 1875], for finding new integral solutions of the equation (7) clearly suggests its geometrical meaning. Equality (11) puts a straight line in homogeneous projective coordinates X, Y, Z that passes through the known points (x, y, z) and (x_1, y_1, z_1) of the cubic (7). The new solution (X, Y, Z) thus represents a third point of intersection of this straight line and the cubic (7). But geometrical formulations of the methods are absent in [Lucas 1875] and [Lucas 1877]. They were given in [Lucas 1878], which also included the general equation (6) (see above). In the same article, Lucas noted that “*la méthode donnée par Cauchy pour l’équation $Ax^3 + By^3 + Cz^3 = 3Dxyz$ revient au second [procédé]*”, *i.e.*, to the secant method [Lucas 1878, p. 508].

In a 1879 article published in the *American Journal of Mathematics*, Lucas once again gives the geometrical formulation of the problem

of solving the indeterminate equation (6) and the tangent, secant and conics methods [Lucas 1879], repeating the corresponding passage from [Lucas 1878] word for word. Supplementing his exposition with an historical excursus, he gives the formulae for finding a new rational solution (X, Y, Z) of the equation (7), namely (13), which he attributes to Lagrange and Cauchy, and (8) with reference to [Cauchy 1826]. Lucas remarks [1879, p.180], that the formulae (13) “*peuvent être remplacées*” by the relations (9)–(10), and the formulae (8) by the relations (11)–(12), *i.e.*, by the relations from [Lucas 1875]. Having formulated the procedures of obtaining rational solutions of the equation (6) by means of drawing a tangent, a secant or a conic section, he writes that Lagrange’s and Cauchy’s methods for the equation (7) “*reviennent aux deux premiers procédés*” [Lucas 1879, p. 181]. Thus, in [Lucas 1878]; [Lucas 1879], Lucas clearly singled out *three principal procedures of finding rational points on a cubic curve, to which all previous methods* (based on the application of different linear and quadratic substitutions for solving indeterminate third degree equations), *were reduced*.

One can suppose that Lucas, who knew [Cauchy 1826], came to his procedures through a geometrical interpretation of Cauchy’s methods. Indeed, these methods are presented in [Cauchy 1826] in such a way, that their geometrical meaning is quite obvious, especially for the method corresponding to drawing a secant. But Lucas does not mention these methods for (6), noting only a particular case of (7). Taking into account the analysis of Lucas’s publications carried out above, it seems probable that Lucas paid attention, first of all, to Cauchy’s methods for (7) and then, having discovered their geometrical meaning, generalized these methods in their geometrical formulation to (6). Of course, Lucas might have arrived at his geometrical procedures without depending on Cauchy’s results, but this seems unlikely.

As noted, Lucas’s works on indeterminate equations often contain information of an historical nature. The titles of his works [Lucas 1873; Lucas 1877] also testify to his interest in the history of Diophantine analysis and in the heritage of mathematicians of the past. Lucas was a member of the French Commission dealing with the publication of Fermat’s collected works. In the preface to [Lucas 1873], which was republished in 1961, Jean Itard writes that Lucas would have seen this

publication through had he not died in 1891 at the age of 49 as a result of an accident; instead, the project was completed by Paul Tannery and Charles Henry. (On Lucas and his results in other areas of the number theory, see [Décaillot 1998]; on his mathematical work in general see [Harkin 1957].)

Lucas was not the only one to be interested in the geometrical treatment of indeterminate equations. Even before Lucas published his 1878 paper, Sylvester had, independently from the Cauchy-Lucas tradition, searched for geometrical methods of solving third degree indeterminate equations. Two papers of Sylvester, respectively published in 1847 and 1858, touch upon the questions connected with the geometrical interpretation of such equations. We will extensively come back to Sylvester's methods in the next section of the paper. Let us give here a short description of the contents of the two early papers. In the first paper, Sylvester [1847c] considers the equation

$$(15) \quad x^3 + y^3 + Az^3 = Mxyz$$

with integers A and M , and describes a certain infinite algebraic procedure, with the help of which, under certain conditions on the coefficients A and M , all the integer solutions of (15) can be derived from one solution. Expressing at the end of the paper a supposition that the conditions on A and M can be weakened, Sylvester clearly connects the question about integer solutions of (15) with the properties of the curve

$$(16) \quad Y^3 + X^3 + 1 = \frac{M}{A^{1/3}}XY$$

[Sylvester 1847c, p. 470]. Note that equation (15) interprets in Cartesian coordinates the curve $X_1^3 + Y_1^3 + A = MX_1Y_1$ and this may be transformed by the formulae $X_1 = A^{1/3}X$, $Y_1 = A^{1/3}Y$. The 1858 paper concerns the arbitrary solution $x = a$, $y = b$, $z = c$ of a general homogeneous equation of third degree

$$(17) \quad f(x, y, z) = 0,$$

and offers algebraic considerations, as well as a geometrical treatment. In particular, Sylvester turns to the geometrical interpretation of the problem of solving (6) in integers as a problem of finding points with

integer coordinates on a cubic curve, set by (6).⁷ In [Sylvester 1858], the author informs that he possesses some “doctrine of derivation” of points on a cubic curve, and in particular, of rational points (see below). In conclusion, he expresses his hope “to have tranquillity of mind ere long to give to the world his memoir, or a fragment of it, *On an Arithmetical Theory of Homogeneous and the Cubic Forms*” [Sylvester 1858, p. 109] and adds that “the germ” of it first dawned upon his mind years earlier. But Sylvester did realise his intention only in [Sylvester 1879/80], where his theory is stated in detail.

3. THE STRUCTURE OF THE SET OF RATIONAL POINTS ON A CUBIC CURVE: SYLVESTER

As detailed above, Sylvester’s paper [Sylvester 1879/80] contains the first attempt to study the structure of the set of rational points on elliptic curves by means of the theory of algebraic curves. This interesting fact in the history of Diophantine analysis was noted by Lavrinenko [1982], and Sylvester’s work was also briefly considered in [Schappacher 1991]. This section recasts and expands the analysis given in [Lavrinenko 1982].

J.J. Sylvester was one of the 19th-century mathematicians, who “present the transitional type between the encyclopaedists of the previous century and the particular specialists of our time” [Dahan-Dalmédico and Peiffer 1986, p. 55]. Although his discoveries fall in several fields of mathematics, he was most famous for his results in algebra and especially in the theory of invariants. [Sylvester 1879/80] highlights yet another facet

⁷ His letter to Arthur Cayley of 23 October 1856 shows that Sylvester used such an interpretation earlier as well. In sketching his opinions on the connection between the solution in rational numbers of ternary cubic form equations and of quaternary ones, he writes: “If we have a Cubical Surface with one rational point, tangentialization will give an indefinite number of Rational Curves and thus if I can prove that from a known solution of $x^3 + y^3 + Az^3 + Bt^3 = 0$ I can get a point among the infinite succession of rational curves deducible from it for which $t = 0$, I have solved $x^3 + y^3 + Az^3 = 0$ ” [Parshall 1998, p. 93]. Parshall, commenting on Sylvester’s letter, notes that “here, he thinks he has hit upon a technique for finding integral solutions of equations of the form $x^3 + y^3 + Az^3 = 0$. [...] As his published works of 1856 to 1859 make evident, Sylvester did not get very far with this entire line of research” [*Ibid.*]. In the context of the present argument, it is important to note that Sylvester not only freely uses geometrical language when treating indeterminate equations but also attempts to investigate these equations by geometrical means.

of Sylvester's research, namely the investigation of rational solutions of Diophantine equations.

A word is in order, first, about Sylvester's earlier publications, dealing with indeterminate third degree equations.

3.1. Sylvester's early publications (1847–1858)

In the 1847 issue of the *Philosophical Magazine*, three papers dealing with indeterminate equations were published by Sylvester. These articles constitute a sort of cycle. The first two deal with the indeterminate equation

$$(18) \quad Ax^3 + By^3 + Cz^3 = Dxyz.$$

In the first paper, Sylvester [1847a] formulates — but does not prove — two theorems on the connection between the solution in integers of equation (18) under certain conditions on the coefficients A, B, C, D and the solution in integers of the equation of the same kind but with coefficients A', B', C', D' connected with A, B, C, D by certain relations. He points out that one can obtain statements about the insolubility in integers of equations (18) as consequences of these theorems, and he gives a number of such statements. He notes as well that, in some cases of solubility in integers of (18), “the general solution can be obtained by equations in finite differences” [Sylvester 1847a, p. 189]. Apparently, Sylvester alludes here to results that he would state in [Sylvester 1847c], and that were mentioned in Section 2 above.

In the second article in the cycle, [Sylvester 1847b], Sylvester formulates the theorem from [Sylvester 1847a] more precisely and states “the Theorem of Derivation” in which formulae are given for obtaining a rational solution of the equation $x^3 + y^3 + ABCz^3 = Dxyz$ from a known rational solution of (18). He also points out cases of the insolubility of $x^3 + y^3 + 2z^3 = Mxyz$ for some values of M , finds several solutions in integers for $M = -2$ with the help of “the Theorem of Derivation”, and gives other examples of applying this theorem to specific equations of the type (18). In the third paper from this cycle, Sylvester [1847c] considers equation (15) and asserts that, under certain conditions on the coefficients A and M , “all the possible solutions in integer numbers of the given equation may be obtained by explicit processes from one particular

solution” [Sylvester 1847c, p. 467], which Sylvester calls “primitive”. The article gives two groups of formulae: the first one expresses a new integer solution through the solution found at the preceding step; and the second one allows to find a new integer solution by the solution found at the preceding step, and by the primitive solution. Sylvester describes the sequence in which these formulae should be used, so that as a result all the integer solutions of the considered equation could be derived. However, he explains neither how these formulae are obtained, nor why the procedure he described gives all the integral solutions of (15).

Interestingly, Sylvester concluded the first article of the cycle with the hope “that as opening out a new field in connexion with Fermat’s renowned Last Theorem, and as breaking ground in the solution of equations of the third degree, these results will be generally allowed to constitute an important and substantial accession to our knowledge of the Theory of Numbers” [Sylvester 1847a, p. 191]. Citing these words and remarking that Sylvester “applied his mathematical energies in 1847 to number theory”, Parshall writes: “It would seem from this that, in hunting for mathematical research problems in 1847, Sylvester had big game — Fermat’s Last Theorem — in his sights. Significant progress on such a famous open problem would certainly have established Sylvester quickly as a mathematician of note” [Parshall 1998, p. 19]. All three articles of 1847 represent, in essence, only a summary of results concerning some classes of indeterminate equations (18) and of particular equations of this kind. However, Sylvester claims that “the proof of whatever has been here advanced exists not merely as a conception of the author’s mind, but fairly drawn out in writing, and in a form fit for publication” [Sylvester 1847b, p. 296]. He apparently never brought this fuller exposition to light.

The same brief account of results concerning indeterminate equations is given in [Sylvester 1856] and [Sylvester 1858]. The former, like the articles of 1847, contains a number of statements concerning the insolubility in integers of certain classes of equations (18). The latter presents a theory of “derivative points” on a cubic, which can also be applied to the problem of integral solutions of the indeterminate equation (6). At first, Sylvester considers a general homogeneous equation of third degree (17) where the requirement that the coefficients and the known solution (a, b, c) of this equation be integers is not specified. He states that he is “in possession of

the equations by means of which” from one given solution a, b, c of (17) new solutions “may be formed explicitly by successive derivation from one another” [Sylvester 1858, p. 108]. He calls solutions obtained in this way “the first or primary, the second, third, etc. derivative systems” and states that “the quantities belonging to the n th derivative” are algebraic functions of degree n^2 of a, b, c . Sylvester revisits this statement, which he later terms “the Law of Squares” [Sylvester 1879/80]. As noted above, in [Sylvester 1858], the author juxtaposes an algebraic and a geometric consideration of the question. Explaining his “Law of Squares”, he gives the following examples of “derivative systems”: 1) the coordinates of the point of intersection of a tangent to a cubic curve at the point (a, b, c) with the curve are biquadratic functions of a, b, c ; 2) “the point in which the conic of closest contact with a cubic curve cuts the curve” has a “derivative system of coordinates” of the 25th degree with respect to the original ones. Turning in the second part of this note to the question on “the connection of this theory of derivation with the arithmetic of equations of the third degree between three variables with integer coefficients”, *i.e.*, equations of the kind (6), Sylvester at first points out that he “ascertained the existence of a large class of equations, soluble, or possibly so, it is true, but enjoying the property that all their solutions in integers, when they exist, are monobasic; that is to say, all their solutions are known functions of one of them, which [he] term[s] the base”.⁸ He further writes: “If this solution be laid down as a point in the curve corresponding to the given cubic, all the other solutions possible in integers will be represented by points on this curve, which are derivatives (in the sense previously employed in this note) to the given point, having coordinates respectively of the 4th, 9th, 16th, etc. degrees, in respect of the coordinates of the basic point” [Sylvester 1858, p. 109]. Sylvester [1858] thus interpreted solving (6) in integers geometrically, and also indicates two geometrical ways of finding such solutions: 1) by drawing a tangent and 2) by drawing a conic of closest contact.

As noted above, the connection between [Sylvester 1858] and “the theory of rational cubic derivation” given in [Sylvester 1879/80] is evident,

⁸ Probably, Sylvester meant the above mentioned results from [Sylvester 1847c], where such equations were considered. These equations are called there ‘monogeneous’, and the initial solution – ‘the base’ in [Sylvester 1858] is called ‘primitive’ in [Sylvester 1847c].

whereas the results in [Sylvester 1847a; 1847b; 1847c; 1856] may not appear at first glance to be connected directly with this theory. In [1858, p. 109] (see the quotation above), however, Sylvester himself pointed to a connection between finding “the derivation points” to a given point on a cubic and finding rational solutions of the so-called “monobasic” equations. He had considered the latter in [Sylvester 1847c]. Still, he appears not to have elaborated further on this asserted connection, unless this remark following the construction of “the natural scale of rational derivatives to a point on a cubic curve” provides a clue [Sylvester 1879/80, pp. 60–61]: “[...] It follows [from the theory of residuation] that by no conceivable geometrical process can any rational point be reached [proceeding from the initial point] not included in the numbered chain [*i.e.*, ‘the natural scale of rational derivatives’], and the inference becomes in the highest degree probable, and, as a matter of fact, is undoubtedly true (although the reasoning upon which it is here made to rest is not absolutely conclusive), that no rational deducts from a general point on a general cubic exist save those that belong to the numbered chain”.

3.2. Sylvester’s memoir on certain ternary cubic-form equations (1879/80)

As for [Sylvester 1879/80], note that by the time it was published its author was serving as the first Professor of Mathematics at the Johns Hopkins University in Baltimore, Maryland, a post he had assumed in 1876. This university, which opened in 1876, was founded as an educational institution of a new type in the United States, namely, “as an institution of higher education devoted to the ideal of research, which would set new standards not only for American higher education generally but also for American mathematics particularly” [Parshall and Rowe 1994, p. 53]. Within this novel setting, Sylvester founded “America’s first school of mathematical research”⁹. (For a detailed consideration of this subject, see [Parshall and Rowe 1994]; [Parshall 1998]).

⁹ It would be interesting to know Sylvester’s impressions of the first months of his stay in the USA in 1876. In his letter to Barbara Bodichon of the 21st of August 1876 he writes: “How unlike America to Europe! much further from us English than are the French, Italians, Germans or Russians although they speak the same language and outwardly follow the same habits; I do not think it possible that I can ever regard America as a home” [Parshall 1998, p. 155]. Did Sylvester think the same when he left Baltimore in December 1883 to take the Savilian chair of geometry at the University of Oxford? Judging by his letters, having learned of his appointment to the chair of Oxford, he “felt a calm as well as a sadness? He was going home to England, but he

Beginning 1878, that research school had at its disposal the pages of the *American Journal of Mathematics*, a journal published under the auspices of the Johns Hopkins University meant to foster research both within university and nationwide. Sylvester, its first Editor-in-chief, “actively solicited papers from mathematicians in the United States and abroad, and worked tirelessly to assure an adequate backlog through his own contributions” [Parshall 1998, p. 160]. Parshall and Rowe note that under Sylvester’s editorship from 1878 to 1884, the journal attracted research of high quality. Among the works published there were articles by Cayley, Clifford, Benjamin Peirce, Charles S. Peirce, and Sylvester himself. During Sylvester’s tenure as editor, roughly one-fourth of all contributions came from foreign mathematicians, and slightly less than half came from within its own institution. According to Parshall and Rowe [1994, p. 93], “the *American Journal*, unlike the many failed American attempts at mathematics journals before it, was a consistently serious, strongly supported research-level mathematics publication”. Among its subscribers were such noted mathematicians as Arthur Cayley in England and Charles Hermite in France.

As the department’s Head Professor at Hopkins, Sylvester “concentrated almost exclusively on his own research and related course work” [Parshall and Rowe 1994, p. 108]. His graduate courses tended to reflect his immediate mathematical interests, namely the theories of invariants, partitions, and algebras, but he used them to draw his students into active mathematical work. Conversely, a student’s question or a discussion could lead Sylvester to new research or to change the subject matter of his lectures (for examples, see [*Ibid.*, pp. 80, 108]). Parshall [1998, p. 159] notes that “Sylvester’s teaching and his research represented mutually reinforcing priorities of his research professorship”. According to [Parshall and Rowe 1994, pp. 109–110], Sylvester turned to the question about rational points on a cubic in [Sylvester 1879/80], “spurred by the year-long course in number theory which he had given for the first time beginning in the fall of 1879”. Apparently, Sylvester discussed in his graduate lectures the questions he ultimately treated in his article; he explicitly mentions results of Fabian Franklin [Sylvester 1879/80, pp. 387, 85–86], a graduate student

was leaving Baltimore and the first real academic home he had ever had” [Parshall 1998, p. 161].

and mathematics fellow at Hopkins from 1877 to 1879, who earned his Ph. D. there in 1880.

Sylvester's lengthy work [1879/80] was published in parts over four issues of the *American Journal of Mathematics* in 1879 and 1880. Just before the publication of Sylvester's work began, Lucas's article, "*Sur l'analyse indéterminée du troisième degré. Démonstration de plusieurs théorèmes de M. Sylvester*" [1879] (recall Section 2 above) appeared in the *American Journal*. [Lucas 1879] is, in fact, a slightly recast version of [Lucas 1878b]. In [Lucas 1879], apart from the geometrical formulation of the problem of solving indeterminate equation (6) in rational numbers and the tangent, secant and conics methods, Lucas considers the particular Diophantine equation

$$(19) \quad x^3 + y^3 = Az^3$$

where A is an integer. He notes that an important contribution to the investigation of this equation was made by Sylvester, who gave the sets of values of A for which this equation is insoluble in rational numbers. Lucas formulates and proves Sylvester's statement.¹⁰ He concludes with the result concerning the solubility of (19), he had published earlier in [Lucas 1878a].

As if taking the baton from Lucas, Sylvester immediately began publishing his paper about indeterminate equations. In it, he uses geometrical together with traditional algebraic terminology, speaking about rational points on a cubic as well as about rational solutions of a third degree equation. The first chapter of his work deals with equation (19). In the opening pages, Sylvester mentions Lucas's geometrical procedures for deriving new rational points on a cubic curve from known rational points [Sylvester 1879/80, pp. 281–282]. He draws attention to Lucas's method of deriving a new rational point by means of intersections of a cubic curve with a

¹⁰ In 1867 in the *Nouvelles annales de mathématiques* Sylvester had suggested the following statement for the proof: "*p et q désignant des nombres premiers respectivement des formes $18n + 5$ et $18n + 11$, il est impossible de décomposer en deux cubes, soit entiers, soit fractionnaires, aucun des nombres suivants: $p, 2p, 4p^2, q^2, 2q^2, 4q$* " [Sylvester 1867]. This statement had actually already been proved by T. Pépin in 1870 (see [Dickson 1920, p. 574]), but Lucas, apparently, did not know this when his article was published. T. Pépin also gave other values for A , for which (19) is insoluble in rational numbers.

conic and points out that this method “amounts only to a combination of the other two” (*i.e.*, of the secant and tangent methods). In the paper’s next installment, Sylvester considers the question of rational solutions of the equation $x^3 - 3xy^2 - y^3 + 3z^3 = 0$, noting that “in general, (except at points of inflexion or at points whose i th tangentials are points of inflexion¹¹), one rational point in a cubic gives rise to an infinite series of rational derivatives” [Sylvester 1879/80, p. 381]. By “rational derivatives” of a point on a cubic, he means points, that can be obtained from this point with the aid of various combinations of the secant and tangent methods.

Finally, in the paper’s third installment, Sylvester begins to state his “theory of rational derivation” in his “Excursus B. On the Chain Rule of Cubic Rational Derivation”. He considers an arbitrary cubic curve on the projective plane and investigates the set Ω of “rational derivatives” of a point on this curve. Here, he does not restrict himself to initial points with rational coordinates. Still, as noted, the problem of studying the set Ω appeared in [Sylvester 1879/80] in connection with his investigations of Diophantine equations and, so, initially for the case, when an initial point is rational. Perhaps, because the rationality requirement is absent, Sylvester’s results on the structure of the set Ω from “Excursus B” are not even mentioned in such a comprehensive work as Dickson’s *History of the Theory of Numbers*. Dickson notes only the formulas given in [Sylvester 1879/80] for coordinates of a point obtained by means of the tangent method or of the secant method from one or two known points [Dickson 1920, p. 591]. Let us consider the subject of “Excursus B” in more detail.

3.3. The “natural scale of rational derivatives” to a point on a cubic curve

Sylvester calls finding a new point Q on a cubic from a known point P by means of the tangent method, “the tangentialization”, and the point Q obtained is “the tangential” to the point P . The point R obtained by the tangentialization from the point Q is called the second tangential to the point P , and so on. Finding a new point on a cubic from two known points by the secant method is called “the collineation”, while the new point is called “the collinear to given points” or “their connective”. We also use this terminology.

¹¹ These are not all the cases in which the set of “rational derivatives” to some point on a cubic may be finite. On this, see §3.3 below.

Sylvester writes: “Let us take any point on a cubic curve along with its successive tangentials ad infinitum. We may, by drawing straight lines through any two of these points, either contiguous or apart, to meet the curve, obtain an additional set of points, and thus form an enlarged system which may again be subjected to a like process of collineation or tangentialization, and such method of augmentation and amplification may be continued indefinitely. Every point thus obtained will obviously be a rational derivative of the original point (*i.e.* its co-ordinates will be rational integral functions of those of that point) [...]” [Sylvester 1879/80, p. 58].

Sylvester’s algorithm for obtaining rational points

In his work, Sylvester gives a simple algorithm for obtaining the points in the set Ω produced by one rational point. Simultaneously, he establishes some properties of Ω . Let us consider this algorithm.

First of all, Sylvester introduces the notation $(m, n) = p$ or $m, n = p$, meaning that the point p is found from points m and n by the secant method. Clearly, if $(m, n) = p$, then $(m, p) = n$ and $(n, p) = m$. Sylvester denotes the original point P_1 by 1, and its first and second tangentials by 2 and 4, respectively. Therefore, $(1, 1) = 2$, $(2, 2) = 4$, $(1, 2) = 1$, and $(2, 4) = 2$. Sylvester further produces a set of points by means of the secant method using natural numbers to denote the points obtained: $1, 4 = 5$; $2, 5 = 7$; $1, 7 = 8$; $2, 8 = 10$; $1, 10 = 11$; $2, 11 = 13$; and so on. He remarks in a footnote that sometimes it will be “more convenient to use $P_1, P_2, \dots, P_n; P'_1, P'_2, \dots, P'_n$ in lieu of $1, 2, \dots, n; 1', 2', \dots, n'$ ”. He obtains this sequence in the following way:

$$(20) \quad (1, 3k + 1) = 3k + 2, \quad (2, 3k + 2) = 3k + 4, \quad k = 0, 1, 2, \dots$$

to get

$$(21) \quad 1, 2, 4, 5, 7, 8, 10, 11, 13, \dots, 3k + 1, 3k + 2, 3k + 4, 3k + 5, \dots$$

or all natural numbers not divisible by 3. Sylvester calls these numbers the indices of the corresponding points. The process of building the sequence (21) involves determining a new point at each step as a result of applying the secant method to the point 1 or 2 and to the point found in the previous step. All the other elements of Ω can be found by applying,

in all possible ways, the secant and tangent methods to the points of sequence (21) and to the new points found. This seemingly represents an infinite process “of augmentation and amplification”, analogous to finding Ω based on the set of tangentials, which Sylvester described in [Sylvester 1879/80, p. 58] (see the quotation above). Yet, what does Sylvester do? He first proves the following theorem:

If natural numbers m and n are not divisible by 3 and $m > n$, then

$$(m, n) = \begin{cases} m - n & \text{if } m - n \text{ is not divisible by 3,} \\ m + n & \text{if } m + n \text{ is not divisible by 3.} \end{cases}$$

The following fact from the theory of algebraic curves underlies the proof of this theorem: for any four points on a cubic curve

$$(A) \quad (a, b), (c, d) = (a, c), (b, d).$$

In other words, if four points on a cubic are paired in any way, the connective of the connectives of the points in the separate pairs is independent of the manner of grouping.¹² Sylvester refers his readers to the exposition of the theory of residuation found in [Salmon, 1879] for this fact. To prove the theorem, Sylvester considers four cases differing in what the remainders from the division of the numbers m and n to 3 are. Denoting the indices of the points not by m and n but by r and s , Sylvester supposes, in the first case, that $r = 3i + 1$, $s = 3j + 1$, $j - i > 0$ and writes down a sequence of equalities:

$$r, s = (3i - 1, 2)(3j + 2, 1) = (3i - 1, 1), (3j + 2, 2) = 3i - 2, 3j + 4 = r - 3, s + 3$$

using (A) as well as the definitions (20) and the fact that if $(m, n) = p$, then $(m, p) = n$ and $(n, p) = m$. To complete the proof of the first case, Sylvester notes that from the equality $r, s = r - 3, s + 3$ it follows that $r, s = r - 3i, s + 3i$, and $r - 3i, s + 3i = 1, s + r - 1 = s + r$. The other three cases follow similarly.

From this theorem, it follows that the set of points (21) is closed with respect to “collineations” and “tangentializations”, that is, the secant and

¹² Can the rule (A) be considered as some ‘variante’ or ‘analog’ of the property of associativity? In our opinion, it is rather a special property of the introduced operation having no direct relation to the property of associativity.

tangent methods applied to the points (21) give us the points of this sequence once again. Therefore, the sequence (21) already contains all the points of the set Ω ! Sylvester calls it “the natural scale of rational derivatives to a point on a cubic curve” [Sylvester 1879/80, p. 58]. Since this set is closed, he also calls it “a self-contained group” [*Ibid.*, p.61].

Sylvester’s theorem enables us to ascertain how to obtain a certain point of the sequence (21). Sylvester gives the following example: according to the theorem, $4, 4 = 8$, and according to the definition $8 = 1, 7 = 1, (2, (1, 4))$. From this, he concludes that it is possible to find the third tangential “when a point on a cubic and its first and second tangentials are given, by collineation alone” [Sylvester 1879/80, pp. 59–60]. He also notes that “the tangential of the i th order” to the point 1 has the index 2^i (this follows easily from the stated theorem), so that the set of all indices of the kind 2^i , $i \in \mathbb{N}$, corresponds to the set of “tangentials” to the point 1 [*Ibid.*, p. 60].

Thus, Sylvester carried out the first systematic investigation of the structure of the set Ω , by introducing the notion of the index of a point in Ω and by operating not with the points’s coordinates but with their indices. He determined the index of the rational points on a cubic obtained by the tangent or secant method from any points with known indices. It thus followed that two different combinations of the secant and tangent methods could lead to the same result. His rule for operating with indices made it possible to determine exactly how to obtain a point with the given index and how to find Ω .

The connection with elliptic arguments

The connection between Sylvester’s use of indices and the use of elliptic arguments of points on a cubic in the modern arithmetic of elliptic curves is clear. Indeed, if a cubic curve is given in the usual Weierstrassian form

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

then the sequence regarded by Sylvester can be given by means of the elliptic arguments of the curve’s points. Let α be the elliptic argument of the original point 1. It is easy to check that according to the definitions (20), the following elliptic arguments

$$(22) \quad \alpha, -2\alpha, 4\alpha, -5\alpha, 7\alpha, -8\alpha, 10\alpha, -11\alpha, 13\alpha, \dots$$

correspond to the points of the sequence (21). Thus it is enough to consider that the equality $\alpha + \beta + \gamma = 0$ is true for the elliptic arguments α, β, γ of three collinear points on a cubic. This yields the sequence $(3k + 1)\alpha$, $k = 0, -1, 1, -2, 2, -3, 3, \dots$

Comparing the sequence (21) of indices of points with the sequence (22) of elliptic arguments of the same points, we see immediately that Sylvester's indices are simply absolute values of the coefficients of the elliptic arguments of the corresponding points! It was just this sequence (22), that Poincaré considered in [1901], introducing the set of rational points generated by a known rational point. If the secant method is applied to the points of the sequence (22) with arguments $(3m + 1)\alpha$ and $(3n + 1)\alpha$, the point with argument

$$-(3m + 1)\alpha - (3n + 1)\alpha = (-3m - 3n - 2)\alpha = (-3(m + n + 1) + 1)\alpha,$$

will be obtained, again belonging to (22). It is not hard to show that this result is equivalent to Sylvester's theorem. Let us emphasize that Sylvester developed his theory of indices without mentioning either elliptic parameters of points or the correspondence between them and indices. Could he have been aware of this correspondence? This suggestion provides a reasonable explanation for how Sylvester managed to introduce such a felicitous numeration of the points of Ω , a numeration, that suggests simple rules for operating with indices. While reasonable, this suggestion is unlikely. If one proceeds initially from the elliptic parameters, then it is more logical to determine the index of a point as a coefficient at α , and not as its absolute value. Thanks to such a definition, a full analogy between operations with indices and operations with elliptic parameters is established, and rules for operating with indices are considerably simplified (especially for the points from the set Ω_1 , which will be considered below). This way is exactly how the American mathematician, William Story, proceeded; we consider his work in section 4 below. But if Sylvester's theory of indices was created without any connection with the use of elliptic parameters, then how can we explain the correspondence between parameters and indices, which at first sight seems so surprising? Apparently, both the theory of indices and elliptic parameters provide means of describing the structure of one and the same set, namely the set of points of a cubic generated by a single point by means of the tangent

and secant methods. Though these means of description are obtained differently, they both reflect the structure of one and the same set, and their closeness seems to be quite natural.

3.4. The “completed scale of rational derivatives” to an arbitrary point on a cubic

Sylvester did not stop with this consideration of the set Ω . He actually completed his “scale of rational derivatives” by means of an arbitrary known point I of inflexion on a cubic curve in the following way. Sylvester calls the two points on a cubic that are collinear with I “opposite”. The point opposite to the point from Ω is denoted by the same index, but accented, *i.e.*

$$(23) \quad p' = (I, p)$$

where p is an index of the point from Ω . Sylvester remarks that $(I, I) = I$, $(p', p) = I$, $(p')' = p$ and proves that $(p', q)' = p, q'$. Although he does not establish the equality $(p', q') = (p, q)'$ (which can be proved similarly to the previous one), he uses it subsequently. Then, using the point $1'$, he determines the points with indices divisible by 3:

$$(24) \quad 1', 2 = 3; \quad 1', 5 = 6; \dots; \quad 1', 3i - 1 = 3i; \dots$$

He finally introduces a system consisting of the points $1, 2, 3, 4, 5, 6, 7, 8, \dots$ and their opposites, which he calls “the completed scale of rational derivatives to an arbitrary point on a cubic” [Sylvester 1879/80, p. 68]. Let us denote this system of points by Ω_1 . Sylvester notes that the coordinates of these new points are rational functions of the coordinates of the original point 1 and the point I of inflexion. This follows from the formulae of the secant method, which Sylvester gets in [1879/80] in the same way as Cauchy.

After introducing the system

$$(25) \quad \begin{cases} 1, 2, 3, \dots, n, \dots, \\ 1', 2', 3', \dots, n', \dots, \end{cases}$$

Sylvester [1879/80, p. 69] asserts that “the connective of any two points in the double chain [*i.e.* in the system (25)] may be expressed as a single

point therein”, *i.e.*, the system (25) also has the “surprising” property of being closed with respect to collineations and tangentializations. Note that this statement is not absolutely correct, since the connective of any two opposite points p and p' from (25) is a point of inflexion I . Therefore, the system will be closed with respect to collineations and tangentializations only if the point of inflexion I with the index 0 is added to this system. Essentially, it is precisely this fact that Sylvester establishes, obtaining rules of operating with indices of points from the system (25) at collineations. To do this, he considers a number of cases differing in what the remainders from the division of the indices to 3 are and whether or no they have accents. For example, if $r = 3i + 1$, $s = 3j + 1$ and $s \geq r$, then $r, s' = s - r$ and $r', s = (s - r)'$; if $r = 3i + 2$, $s = 3j + 2$ and $s \geq r$, then $r, s' = (s - r)'$ and $r', s = s - r$; if $r = 3i + 1$, $s = 3j - 1$, then $r, s' = (r + s)'$, and so on.

Skillful use of (A) for points on a cubic curve, of the definitions (20), (23), and (24) for indices, and of obvious properties of collineations characterize Sylvester’s proofs for the rules of operating with indices. For example, proving the equality $3i + 1, (3j + 1)' = 3j - 3i$ in the case where $i \leq j$, Sylvester first obtains $3i + 1, (3j + 1)' = 3i - 2, (3j - 2)'$, concludes that

$$3i + 1, (3j + 1)' = 1, (3j - 3i + 1)',$$

and then writes down a sequence of equalities

$$\begin{aligned} 1, (3j - 3i + 1)' &= (1, 2), [(3j - 3i - 1)', 2'] \\ &= (2, 2'), [1, (3j - 3i - 1)'] = 1', 3j - 3i - 1 = 3j - 3i. \end{aligned}$$

In more detail:

$$\begin{aligned} 1, (3j - 3i + 1)' &= (1, 2), (3j - 3i - 1, 2)' = (1, 2)[(3j - 3i - 1)', 2'] \\ &= (2, 2'), [1, (3j - 3i - 1)'] = I, [1, (3j - 3i - 1)'] \\ &= [(1, (3j - 3i - 1)')] = 1', 3j - 3i - 1 = 3j - 3i. \end{aligned}$$

In this proof, apart from (A) and definitions (20), (23) and (24), Sylvester used the following properties of collineations:

$$1 = (1, 2); \quad (p, q)' = (p', q'); \quad (p, p') = I; \quad (p, q)' = p', q.$$

Translating Sylvester's results into language we are accustomed to, let the cubic curve be given in the normal Weierstrassian form. The infinite rational point $(0 : 1 : 0)$ of this curve is a point of inflexion, which we will take as the point I . Introducing it to the system (21) corresponds to introducing 0 to the system (22). The point opposite, in Sylvester's sense, to the point with elliptic argument $n\alpha$ has elliptic argument $-n\alpha$ (since it is equal to $-(n\alpha + 0)$). Thus, it is opposite in the modern sense as well. Procedure (24) consists of obtaining the points with elliptic arguments $3i\alpha$, $i = 1, 2, \dots$. Indeed, the point with index $1'$ has argument $-\alpha$, and the point with index $3i - 1$ has argument $-(3i - 1)\alpha$ (compare (21) and (22)). The point with argument $-(-\alpha - (3i - 1)\alpha) = 3i\alpha$ is found from these points by the secant method. Therefore, the sequence (25) of indices of the considered points corresponds to the following sequence of elliptic arguments of these points:

$$(26) \quad \begin{aligned} & \alpha, -2\alpha, 3\alpha, 4\alpha, -5\alpha, 6\alpha, \dots, -(3k - 1)\alpha, 3k\alpha, (3k + 1)\alpha, \dots, \\ & -\alpha, 2\alpha, -3\alpha, -4\alpha, 5\alpha, -6\alpha, \dots, (3k - 1)\alpha, -3k\alpha, -(3k + 1)\alpha, \dots \end{aligned}$$

Indices (disregarding the accent) are thus simply absolute values of coefficients by α in the elliptic arguments of the considered points. If the initial point (with index 1 and with the elliptic argument α) is rational then the set Ω_1 studied by Sylvester is, in modern terms, simply the subgroup of the group of rational points on a cubic generated by one rational point (namely, by the point with the elliptic argument α). Sylvester, however, did not recognize that a group structure was possible on the set Ω_1 ; his binary operation $(.,.)$ was not a group operation.

It is not hard to check that the rules Sylvester obtained for operating with indices (25) correspond to the rule for operating with elliptic arguments under collineations. However, the rules for indices are more cumbersome, since account has to be taken of whether the indices are accented and of what the remainders are after division of the indices by 3. Sylvester remarks that in all these cases "the connective of two indices (disregarding the accent) is either their sum or their difference" [Sylvester 1879/80, p. 70]. It would only have remained for him to ascribe a negative sign to certain groups of indices in order to get the common rule that applying the secant method to two indices yields their sum taken with the opposite sign (the same thing as for the elliptic arguments). However, he did not do this.

Sylvester also touched on some other questions connected with the investigation of the set (25). For instance, he established which points are obtained if an arbitrary point of the set (25) is taken as an original point in the procedure of building “the completed scale of rational derivatives”. The rules giving indices of the points of this scale correspond to analogous rules for elliptic arguments. Essentially, Sylvester considers here a cyclic subgroup of the group Ω_1 generated by an arbitrary element of Ω_1 .

3.5 The case of the finiteness of “scales”

Sylvester also points out, in [Sylvester 1879/80], that “the natural scale of rational derivatives” (21) and “the completed scale of rational derivatives” (25) to a certain point on a cubic can be finite. Even before stating the general theory of “cubic rational derivation”, Sylvester considers the equation

$$(27) \quad x^3 - 3xy^2 - y^3 + 3z^3 = 0$$

for which he specifies three integer solutions: $(1 : 1 : 1)$, $(-2 : 1 : 1)$ and $(1 : -2 : 1)$ [Sylvester 1879/80, p. 381]. Sylvester points out that although in general “one rational point in a cubic gives rise to an infinite series of rational derivatives”, this does not occur in this case, since points $(1 : 1 : 1)$, $(-2 : 1 : 1)$ and $(1 : -2 : 1)$ are the apices “of a triangle in-and-exscribed to the curve $x^3 - 3xy^2 - y^3 + 3z^3$ ” and each of these points is its own third tangential. By the triangle “in-and-exscribed to the curve”, Sylvester understands the triangle ABC , the apices of which lie on the curve with AB touching the curve at the point A , BC at B , and CA at C . In other words, the apices of such a triangle are the point A and its first and second “tangentials” (the points B and C), the third “tangential” of the point A coinciding with the point itself. (In Sylvester’s example, a simple check shows that the point $(-2 : 1 : 1)$ is a “tangential” to the point $(1 : 1 : 1)$, the point $(1 : -2 : 1)$ is a “tangential” to the point $(-2 : 1 : 1)$, or the second “tangential” to the point $(1 : 1 : 1)$, and the point $(1 : 1 : 1)$ is a “tangential” to the point $(1 : -2 : 1)$, or its own third “tangential”). Therefore, applying the tangent or secant method to any of these points yields one of these points, and “the scale of rational derivatives” (21) to any of these points on the curve (27) is finite and consists of three points.

In the same paragraph, Sylvester points out that a cubic given by the equation

$$x^2y + y^2z + z^2x + \lambda xyz = 0,$$

will be “in-and-exscribed” to the triangle with the sides $x = 0$, $y = 0$ and $z = 0$. It is not difficult to establish that the apices of this triangle are the points $(0 : 0 : 1)$, $(0 : 1 : 0)$, $(1 : 0 : 0)$, which belong to the curve under consideration. Any of these points is its own third “tangential”, and two other points are its first and second “tangentials”. Therefore, as in the previous example, “the scale of rational derivatives” (21) to any of these points will consist of these three points.

After constructing “the natural scale of rational derivatives” (21) in “Excursus B”, Sylvester also considers the case when that scale is finite [Sylvester 1879/80, p. 61], in which case the set contained in (21) of all the successive “tangentials” to the initial point should be the same. He indicates two cases where this happens: 1) when “for some number i the i th tangential coincides with the initial point”, and 2) when “a tangential of some order shall fall upon a point of inflexion” and, consequently, “the succeeding tangentials remain fixed at that point” [Sylvester 1879/80, p. 61]. Sylvester points out that “these are obviously necessary conditions of the chain [*i.e.* ‘the natural scale of rational derivatives’] being finite”, and while it remains to show that they are sufficient, “that will best appear after the theory of derivation from a general point combined with a point of inflexion has been discussed” [*Ibid.*]. Note that Sylvester indicated two cases, in which the set of all “tangentials” to a point on a cubic is finite, but overlooked the third case, where for some number i the i th tangential coincides not with the initial point but with one of the obtained “tangentials”. The latter is precisely the case, when the point is of the 10th order: it is not difficult to check that the fifth “tangential” to this point coincides with its first “tangential”, while no “tangential” to this point coincides with the point itself.

Sylvester asserts that, in the first case, when some “tangential” coincides with the initial point, “the chain forms a closed polygon”, and in the second case, when some “tangential” coincides with a point of inflexion, “the chain is an open but finite one”. Apparently, “the chain” here refers not to the whole “scale of rational derivatives” (21) but only to the initial

point with its successive “tangentials”, for in the first case it is this set and not the sequence of points (21) that forms a closed polygon.¹³

Sylvester considers questions connected with the finiteness of “the natural scale of rational derivatives” (21) and “the completed scale of rational derivatives” (25) in the section of “Excursus B” entitled “On Pertactile or Periodic Points on a Cubic Curve” [Sylvester 1879/80, pp. 74–81]. This section deals with the solution of two problems from the theory of algebraic curves, which bear no relation to the investigation of the set of rational points on these curves. The first problem consists of the calculation of the number of pertactile points¹⁴ of given grade i on a cubic, the latter of the calculation of the quantity of “in-and-exscribed k -laterals” for a general cubic.¹⁵ Interestingly, to solve them, Sylvester uses the “theory of rational derivation” he originally developed in the context of Diophantine equations. Although further discussion of these problems is beyond the scope of the present study, their solution appears to be closely connected with the study of the structure of the sets Ω and Ω_1 , *i.e.*, “the natural scale” and “the completed scale of rational derivatives to a point”, which do concern us here.

Sylvester [1879/80, p. 74] first states that:

If the i th derivative of the initial point P_1 is a point of inflexion, which may be any of the nine points of inflexion on a cubic, then $P_{3i-1} = P_1$.

Then proves the converse, namely:

¹³ For example, if the initial point P_1 is the point of the 5th order then it coincides with its fourth tangential and, consequently, the point P_1 with its successive tangentials forms a closed quadrangle. However, it is not difficult to check that, when finding the points of the sequence (21), we successively obtain the points P_1, P_2, P_4, P_5, P_7 (all of them different), and then the same points in the reversed order: P_7, P_5, P_4, P_2, P_1 , then P_1, P_2, P_4, P_5, P_7 , and so on.

¹⁴ Sylvester considers points on a general cubic “at which the cubic admits of a higher order of contact with another curve than in general possible” [Sylvester 1879/80, p. 74]. He writes that “in general, a curve of the i th order can only be made to pass through $3i - 1$ consecutive points situated at P [P is a point on the cubic]” [*Ibid.*]. And if “the $3i$ th point [of intersection of such curve and the cubic] will coincide with P , so that such curve[s] will pass through $3i$ consecutive points”, then “ P may accordingly be termed a point of pluperfect tactility” [*Ibid.*]. Sylvester also terms such a point P a pertactile point of the grade i .

¹⁵ An “in-and-exscribed k -lateral” is a polygon, the apices of which belong to the cubic and have the property that eventually each is a tangential to the previous one. If we take any apex of such a polygon, then all the other apices are $k - 1$ successive “tangentials” to the given apex and its k th “tangential” coincides with it.

If $P_{3i-1} = P_1$, then P_i is a point of inflexion, “which may either be the point used to form the scale, or any of the eight other inflexions” [Sylvester 1879/80, p. 75].

His proof hinges on the rules of operating with indices.¹⁶ Note, too, that these rules readily yield a proof of his first statement. Thus, one can assert that:

$P_{3i-1} = P_1 \Leftrightarrow P_i$ is a point of inflexion.

Sylvester also establishes that if $P_{3i-1} = P_1$, then P_{3i} is I , the original inflexion (*i.e.*, the point of inflexion used to form “the completed scale” Ω_1) and for all $k = 1, 2, \dots, 3i - 1$,

$$(B) \quad \begin{cases} P_k = P_{3i \pm k} & \text{if } k \text{ is not divisible by } 3, \\ P_k = P_{3i+k} = P'_{3i-k} & \text{if } k \text{ is divisible by } 3. \end{cases}$$

From this¹⁷ he concludes that if $P_{3i-1} = P_1$, then “the natural scale $P_1 P_2 P_4 P_5 \dots$ and the completed scale $\begin{cases} P_1 P_2 P_3 P_4 P_5 P_6 \dots \\ P'_1 P'_2 P'_3 P'_4 P'_5 P'_6 \dots \end{cases}$ are each of them

periodic, the period of the indices being $3i$ ” [Sylvester 1879/80, p. 77]. In other words, these scales contain only a finite number of different points. Let us note that the equalities (B) ascertain not only the fact that the process of obtaining the points of “the natural scale” Ω and of “the completed scale” Ω_1 become cyclic (since $P_{3i+k} = P_k, k = 1, 2, \dots, 3i - 1$), when $P_{3i-1} = P_1$. They give a more detailed description of the structure of these scales. For example, if $P_{11} = P_1$, that is if $i = 4$, then, according to the equalities (B), while obtaining the points of “the natural scale” Ω we will subsequently be getting the points $P_1, P_2, P_4, P_5, P_5, P_4, P_2, P_1$, then again this same sequence: $P_1, P_2, P_4, P_5, P_5, P_4, P_2, P_1$, and so on.

Sylvester next considers the problem “of in-and-exscribed k -laterals”, using the fact — which he does not prove, owing probably to its simplicity — that if $P_{3i+1} = P_1$, then $P_{3i-1} = P_1$. (For the proof, it is enough to write down that $P_{3i-1} = (P_2, P_{3i+1}) = (P_2, P_1) = P_1$.) It follows that in the case when $P_{3i+1} = P_1$, the formulae (B) and the statement about the periodicity of “the scales” Ω and Ω_1 remain true.

¹⁶ For example, if $i = 3k - 1$, then $P_i = (P_1, P_{i-1}) = (P_{3i-1}, P_{i-1}) = P_{2i}$, *i.e.* $P_i = (P_i, P_i)$ and this means that P_i is a point of inflexion. The cases $i = 3k + 1$ and $i = 3k$ are similar.

¹⁷ Aside from two obvious misprints, there is a mistake in Sylvester’s demonstration of (B) that can be easily eliminated: he demonstrates that $P_6 = P_{6i+6} = P'_{6i-6}$, while it is necessary to prove that $P_6 = P_{3i+6} = P'_{3i-6}$.

Sylvester's results here can be summarized as follows:

If some point of "the natural scale" Ω , i.e. a point with the index of the kind $3i - 1$ or $3i + 1$, $i \in \mathbb{N}$, coincides with the initial point P_1 (and it occurs if the i th rational derivative of P_1 is a point of inflexion), then the sets Ω and Ω_1 of "the rational derivatives" to the point P_1 consist of a finite number of points.

Thus, [Sylvester 1879/80] provides a sufficient condition for the finiteness of "the natural scale" and "the completed scale of rational derivatives" to a point on a cubic.

Note that it also follows that the conditions of finiteness of "the natural scale" (21), which were considered earlier by Sylvester, are sufficient. Recall that these conditions require that some tangential to the initial point coincides with this point or with a point of inflexion [Sylvester 1879/80, p. 61]. While Sylvester does not mention these conditions here, he remarked earlier — when formulating them as necessary conditions of finiteness of the "natural scale" — that their sufficiency would be established later. He obviously had in mind the results we have just considered.

Sylvester's investigation of the finiteness of the set of "rational derivatives" of a point on a cubic in [Sylvester 1879/80] apparently represents the first attempt to consider this question from a more general point of view. As is well-known, Fermat was able to find from one given rational solution of an indeterminate third degree equation of the types $f_3(x) = y^2$ or $f_3(x) = y^3$ a new one, to iterate this process, and thus to obtain a sequence of rational solutions, generated by one [Fermat 1670, Section 3, §11 and §§22–23]. Referring to Fermat's method in his *Algebra*, Euler wrote that the process of finding new rational solutions can break off, since at some step the solution obtained can coincide with one already found [Euler 1770, Section 2, §113]. Euler gives examples of indeterminate equations, for which the set of rational solutions, obtained by Fermat's method, turns out to be finite [Euler 1770, Section 2, §§121, 155, 156]. Apparently, the more general results on the finiteness of the set of rational solutions, generated by one rational solution of an indeterminate third degree equation, were not known prior to Sylvester's work.

From the modern point of view, Sylvester's "completed scale of rational

derivatives” of a point on a cubic is the cyclic subgroup generated by this point of the group of rational points on a cubic. As is well-known, the cyclic subgroup $\langle a \rangle$ of an arbitrary group $(G, +, 0)$ is finite if the element a has finite order, *i.e.*, if $na = 0$ for some $n \in \mathbb{N}$. Obviously, a is an element of finite order if $ma = a$, for some integer $m \neq 1$. Therefore, the necessary and sufficient condition for the finiteness of the set Ω_1 (*i.e.*, of the cyclic group $\langle P_1 \rangle$) is that some point nP_1 , $n \in \mathbb{N}$, from Ω_1 coincides with the point of inflexion I , playing the role of a neutral element in Ω_1 . Equivalently, some point mP_1 , $m \in \mathbb{Z}$, $m \neq 1$, from Ω_1 coincides with the initial point P_1 .

These conditions — which follow easily in the setting of a group operation of addition of points on the set Ω_1 — are far from evident within the framework of “the theory of indices”, where the indices of points are introduced consequently with the help of three different rules:

$$(P_1, P_{3k+1}) = P_{3k+2}, \quad (P'_1, P_{3k+2}) = P_{3k+3}, \quad (P_2, P_{3k+2}) = P_{3k+4},$$

for $k = 0, 1, 2, \dots$

Nevertheless, Sylvester managed to establish the sufficiency of these conditions, using his rules of operating on indices, although only if the point nP_1 in the first condition has an index from the upper line of the system (25) and the point mP_1 in the second condition belongs to “the natural scale” $\Omega \subset \Omega_1$ (within “the theory of indices” the case, when the point mP_1 , coinciding with the point P_1 , belongs to Ω , — is the easiest). Concerning the first condition it should be specified, that in reality Sylvester ascertained, using the properties of the cubic curve, the sufficiency of a yet weaker condition: if for some $i \in \mathbb{N}$ the point P_i coincides with any of the points of inflexion of the cubic curve (not necessarily with the point I), then the set Ω_1 is finite.

Here, Sylvester’s attempt to investigate these questions in such a general setting and his application of new geometrical ideas for this purpose were perhaps even more important than the results he obtained. Sylvester also gives a purely geometrical characterization of a point on a cubic, “the i th derivative” of which is a point of inflexion and consequently “the natural” and “the completed scales” are finite: this point is “a point of pluperfect tacity of the grade i on a cubic” [Sylvester 1879/80, p. 74].

By considering the finiteness of the sets Ω and Ω_1 in the context of the theory of algebraic curves, Sylvester does not require that the coordinates

of the initial point be rational. He asks questions neither about finding rational points of finite order nor about values the (finite) order of a rational point can take on (*i.e.*, a question about the number of different elements the set Ω_1 may contain). These are 20th-century questions.¹⁸ Just a few years after the publication of [Poincaré 1901], the Italian mathematician, Beppo Levi, made considerable progress in determining the structure of the set of rational points of finite order on an elliptic curve.

4. THE ANALYTICAL APPROACH TO

“THE THEORY OF RATIONAL DERIVATION”: STORY

The above analysis of [Sylvester 1879/80] shows that Sylvester’s use of indices anticipated the application of elliptic arguments of points to the investigation of the structure of the set of rational points on an elliptic curve. As noted, it only remained to change the definition of indices slightly to obtain the complete analogy between acting with indices and acting with elliptic arguments of points. This was actually done in the same year by William Story in his paper “On the Theory of Rational Derivation on a Cubic Curve” [1880, p. 357–365], published in *American Journal of Mathematics*. Parshall and Rowe [1994, p. 109–110] point to the connection between the works of Sylvester and Story, commenting that Story’s paper “largely formed a sequel to Sylvester’s work [...]”. Story sought to recast Sylvester’s number-theoretic approach in a more purely geometrical light by drawing from the researches of Cayley, George Salmon, and Alfred Clebsch in the theory of higher plane curves”. As noted above, however, Sylvester’s work was not purely number-theoretic; he used his theory of indices to solve problems in the theory of algebraic curves. In our view, the merit of Story’s work lays in his combination of

¹⁸ For the solution of the first question, one uses Nagell’s theorem (1935): if (x', y') is a rational point of finite order belonging to the curve $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, then $x', y' \in \mathbb{Z}$ and either $y' = 0$ or $y'^2 \mid (4a^3 + 27b^2)$. The answer to the second question follows from Ogg’s hypothesis, proved by Mazur (1978): a group of all finite order points of an arbitrary elliptic curve over the field \mathbb{Q} is isomorphic to one of the following 15 groups: $\mathbb{Z}/\ell\mathbb{Z}$, $1 \leq \ell \leq 10$, $\ell = 12$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, $1 \leq m \leq 4$. Thus, the order of a rational point, in case the former is finite, can take on the values 1, 2, 3, ..., 10, 12.

the theory of indices with the analytical apparatus of the theory of cubic curves.

Before turning to a consideration of [Story 1880], a few words about its author are in order. William Story (1850–1930) earned his A.B. from Harvard in 1871. From 1871 to 1874, he studied mathematics and physics at Berlin and Leipzig prior to taking his Leipzig doctorate in 1875 for a thesis “On the Algebraic Relations Existing Between the Polars of a Binary Quantic”. In 1876, Sylvester and Daniel Coit Gilman, the first President of the Johns Hopkins University, chose Story for the post of teaching Associate in the Department of Mathematics at Hopkins. As Parshall explains, “the Associate would be responsible for essentially all of the undergraduate teaching, leaving Sylvester free to devote himself to his own researches and to teaching at the graduate level” [Parshall 1998, p. 153]. While thus shouldering most of the department’s teaching burden, Story also picked up the associate editorship of the *American Journal of Mathematics* after its founding in 1878. Clearly then, “Story played a pivotal role in the success of the overall Hopkins program” [Parshall and Rowe 1994, pp. 108–109]. The 1880 article on “rational derivation” on a cubic was Story’s first major contribution to the *American Journal*; he had given graduate lectures at Hopkins on higher plane curves and elliptic functions in 1878–1880. For more on Story and his career, see [Cooke and Rickey 1989]; on his other mathematical results, see [Parshall and Rowe 1994].

In [Story 1880], Story first notes that although “the theory of rational derivation” on a cubic curve was developed “for the purpose of solving an arithmetical problem, [it] has an interest of its own from a geometrical point of view” [Story 1880, p. 356]. He sets out “to develop this new theory of indices in a more general and symmetrical form than that originally given to it; and, finally, by combining it with the theory of parameters, [to] solve a number of problems especially relating to the enumeration of points having certain properties analogous to those of singular points or of the contacts of singular tangents” [*Ibid.*]. Story remarks that “the difference in method of the theories of indices and parameters consists in this: that in the latter continuous values of a parameter are assigned to the continuous points of the curve in accordance with its equation, while in the former to an arbitrary point taken as the initial an index 1 is assigned, and then to its

derivatives in a certain order all positive and negative integers as indices. The index of a derivative thus expresses (with a certain modification due to the inflexion-periods) the number by which the parameter of the initial must be multiplied in order to obtain the parameter of the derivative" [Story 1880, p. 357]. He also supposes that "the parameter μ [is] so chosen, as it always may be, that $\mu + \mu' + \mu'' = 0$ is the condition for three collinear points" [*Ibid.*]. More precisely, for parameters of three collinear points of a non-singular cubic the congruence $\mu + \mu' + \mu'' \equiv 0 \pmod{(\omega, \omega')}$ must hold (see below). As for the construction of "the theory of indices", Story writes: "The condition of collineation above cited must be our guide in the assignment of the indices, in order that the relation mentioned may subsist between index and parameter, *i.e.* for the indices a, b, c of three collinear points the fundamental formula holds, $a + b + c = 0$, or

$$(28) \quad [a, b] = -(a + b)$$

if, in general, $[a, b]$ denote the index of the connective of two points whose indices are a and b " [Story 1880, pp. 357–358]. This approach allowed Story to simplify Sylvester's theory of indices considerably.

So how does Story define indices? He takes first an arbitrary point of inflexion of a cubic and attributes an index 0 to it. Like Sylvester, he considers "the connective" of the chosen point of inflexion and an arbitrary point and calls this the "opposite" to the point. Given a point with the index a , Story assigns the index $(-a)$ to its opposite, *i.e.*, he puts

$$(29) \quad [a, 0] = -a.$$

He also states the following fact from the theory of algebraic curves: the opposites of three collinear points with respect to the same inflexion are also collinear. Therefore, if (28) is true for some a and b , then the equality

$$(30) \quad [-a, -b] = a + b$$

is true as well. Hence, if (28) is true for two points with indices a and b , it is also true for points opposite to them. Story next defines all indices of the form $3m + 1$, $m \in \mathbb{Z}$, attributing to the initial point and to its first tangential the indices 1 and (-2) , respectively, and using these indices alternately for obtaining new indices in accordance with (28):

1 = index of the initial, $[1, 1] = -2$ = index of the tangential of the initial,

$$\begin{aligned} [-2, -2] &= 4; & [4, 1] &= -5; \\ [-5, -2] &= 7; & [7, 1] &= -8; \\ [-8, -2] &= 10; & [10, 1] &= -11; \text{ and so on.} \end{aligned}$$

He also shows that (28) is true for any two indices and that in of the form $3m + 1$, $m \in \mathbb{Z}$. To do this, he uses the same fact from the theory of algebraic curves that underlies all of Sylvester's proofs for rules of operating with indices and that in Story's designations can be represented in this way:

$$(31) \quad [[a, b], [c, d]] = [[a, c], [b, d]] = [[a, d], [b, c]].$$

Story denotes the point $[[a, b], [c, d]]$ (*i.e.*, "the connective of the connectives of the points in the separate pairs") as $[a, b, c, d]$ and calls it "the coresidual" of four given points. His proof is analogous to Sylvester's.

Story notes that "every number of the form $3m - 1$, in which m is any positive or negative integer, is the negative of a number of the form $3m + 1$ " [Story 1880, p. 358]. Therefore, having introduced indices of the form $3m + 1$, $m \in \mathbb{Z}$, Story uses the formula (29) to introduce all the indices of the form $3m - 1$, $m \in \mathbb{Z}$. Rule (28) for points with such indices follows immediately from the fact that they are opposite to the points with indices of the form $3m + 1$. Story also defines "multiples of 3 by the formula $[3m - 1, 1] = -3m$ for all positive and negative values of m , in accordance with the fundamental theorem" [*Ibid.*, p. 360]. Finally, Story proves formula (28) for any two indices a and b , $a, b \in \mathbb{Z}$. He does this, using (31), the definitions of indices, and the rules for operating with them. He first establishes that, for all $a \in \mathbb{Z}$,

$$[a, 1] = -(a + 1), [a, -1] = -(a - 1), [a, 0] = -a.$$

It follows from this that for all $a, b \in \mathbb{Z}$

$$[a, b] = [-a - 1, 1, -b + 1, -1] = [-a - 1, -1, -b + 1, 1] = [a + 2, b - 2].$$

It then only remains to note that this sequence of equalities "can be repeated any number of times until one or the other of the two indices

becomes 0 or 1, in either of which cases the fundamental formula holds; hence it holds for all values of a and b " [Story 1880, p. 360]. From (28) Story obtains, in particular, that "the coresidual of four indices is their sum" [*Ibid.*, p. 361], *i.e.* $[a, b, c, d] = a + b + c + d$.

Thus, owing to the new definition of indices of "the rational derivatives", the theory of indices acquired a simpler and clearer form in [Story 1880]. A set of rules for operating with indices given by Sylvester was replaced by a single rule (28), true for any integer indices a and b . Story essentially simplified the very deduction of rules for operating with indices. Operations with them were brought into line with operations on parameters of points on a cubic curve.

In his work, Story notes that "on a cubic having more than one inflexion, a series of derivatives whose indices are of the form $3m$ and $3m - 1$ exists for each inflexion, and these series determine by collineation yet other series whose indices are of the form $3m + 1$ " [Story 1880, p. 362]. He develops further the theory of indices taking this into account. Thus, for the case of a non-singular cubic with complex coefficients, which generally has nine points of inflexion, he considers series of "derivatives" with indices $a_{p,q}$, where $a \in \mathbb{Z}$, $p = 0, 1, 2$, $q = 0, 1, 2$. Here, he had previously assigned indices of the form $0_{p,q}$, where p and q are as above, to the points of inflexion. In [Story 1880], the rule of operating with such indices was also obtained. Such development of "the theory of rational derivation" was necessary for Story to solve a number of problems from the theory of algebraic curves. He considers these problems explicitly in the second part of the work, where for their solution he applies "the theory of rational derivation" connected with the use of a parametric representation of the cubic curve.

Also in the second part of his work, Story considers a question about the connection between indices and parameters of points on a cubic curve in more detail [Story 1880, p. 368-369]. He investigates the case of a singular as well as of a non-singular cubic. The latter are of particular interest since non-singular cubic curves are precisely elliptic curves of the third order.

Story asserts that the coordinates of any point of a non-singular cubic can be expressed as doubly periodic functions of a single parameter and that this representation seems to be due to Clebsch [1864]. He

also notes that these doubly periodic functions are elliptic and that the simplest representation for a non-singular cubic seems to be the following: $x : y : z = \operatorname{sn} \mu : (\operatorname{cn} \mu \cdot \operatorname{dn} \mu) : \operatorname{sn}^3 \mu$. Story introduces the designations ω, ω' for the periods of the cubic; and (μ) for the point of the cubic, that corresponds to the value of the parameter μ of the parallelogram of periods. The condition that three points $(\mu), (\mu'), (\mu'')$ on a cubic shall be collinear is $\mu + \mu' + \mu'' \equiv 0 \pmod{(\omega, \omega')}$, “*i.e.* the parameters of collinear points satisfy a congruence similar to the equations satisfied by the indices of three collinear derivatives of a common initial. Hence, if a is any integer of the form $3m + 1$, $a_{0,0}$ of $(\mu) = (a\mu)$ ” [Story 1880, p. 368]. From the condition that the parameters corresponding to the inflexions are the solutions of the congruence $3\nu \equiv 0 \pmod{(\omega, \omega')}$, Story finds that $0_{p,q} = (p \cdot \frac{1}{3}\omega + q \cdot \frac{1}{3}\omega')$ and then obtains the formula

$$a_{p,q} \text{ of } (\mu) = \left(a\mu + p \cdot \frac{1}{3}\omega + q \cdot \frac{1}{3}\omega' \right).$$

As he notes further, it follows from this equality that “any point whose parameter differs from an integral multiple of the parameter of a given point by integral multiples of the periods of the inflexions (which are $\frac{1}{3}\omega$ and $\frac{1}{3}\omega'$) is a rational derivative of the given point. In this sense “the theory of rational derivatives is the theory of commensurable parameters” [*Ibid.*, p. 369].

Thus, [Story 1880] establishes the correspondence between the indices of “rational derivatives” of an initial point and elliptic parameters of these “derivatives”. Moreover, if one assigns the parameter 0 to the point of inflexion used for the construction of “the completed scale of rational derivatives”, then the elliptic parameter of the point with index $a \in \mathbb{Z}$, will equal simply $a\mu$, where μ is the elliptic parameter of an initial point. It follows that the set of rational points of a cubic generated by a single rational point, which Sylvester considered in [Sylvester 1879/80], has a simple description by means of elliptic parameters of these points. Thus, the correspondence established by Story pointed to the possibility of an analytical approach to the investigation concerning the structure of the set of rational points on a cubic of genus 1. Sylvester had originally developed his “theory of rational derivation” for this purpose. Story, however, did not consider any questions connected with the study of the set of rational points on a cubic curve in his article.

Today it is usual to reduce the equation of an elliptic curve of third degree to the normal Weierstrassian form $y^2 = x^3 + ax + b$ and to use its parametrization $x = \wp(z)$, $y = \frac{1}{2}\wp'(z)$ with the help of Weierstrass' elliptic function $\wp(z)$. Story, however, uses a different parametrization in terms of Jacobi's elliptic functions. But if from homogeneous coordinates x, y, z of a point in a plane one passes to Cartesian coordinates X, Y according to the formulae $X = x/z$, $Y = y/z$, then Story's parametrization gives

$$X = \frac{1}{\operatorname{sn}^2 \mu}, \quad Y = \frac{\operatorname{cn} \mu \cdot \operatorname{dn} \mu}{\operatorname{sn}^3 \mu}.$$

Since

$$\frac{1}{\operatorname{sn}^2 \mu} = \frac{\wp(z) - e_3}{e_1 - e_3}, \quad \frac{\operatorname{cn} \mu \cdot \operatorname{dn} \mu}{\operatorname{sn}^3 \mu} = -\frac{\wp'(z)}{2(e_1 - e_3)\sqrt{e_1 - e_3}},$$

where $z = \mu/\sqrt{e_1 - e_3}$, there is a simple connection between the parametrization considered in [Story 1880] and that using Weierstrass' function.

Sylvester not only gave a favorable estimation of Story's work but also drew Cayley's attention to it. In a letter to Cayley of 12 May, 1881, Sylvester writes that Story "has a first rate paper coming out in our next number [of the journal] extending and completing my theory of Rational Derivation on Cubic curves — which I think will interest you as he introduces the application of Elliptic Functions to the question" [Parshall 1998, p. 201–202]. Parshall and Rowe characterize Story and his work [Story 1880] well when they write that "unlike Sylvester, who had little patience when it came to reading and absorbing published results, Story revealed himself in this work as a true mathematical scholar capable of fruitfully synthesizing his own ideas and the work of others in the realization of his research objectives" [Parshall and Rowe 1994, p. 110].

Did Poincaré know about [Sylvester 1879/80] and [Story 1880] when he wrote his memoir "*Sur les propriétés arithmétiques des courbes algébriques*" [1901]? He mentions neither Sylvester nor Story nor Hilbert nor Hurwitz, the latter two of whom published results about the set of rational points on curves of genus 0 in 1890, *i.e.*, 11 years earlier than [Poincaré 1901]. Hurwitz [1917, p. 446, note 1] says that Poincaré rediscovered some of their results independently. It seems quite probable that Poincaré did not know of the work of Sylvester and Story. They were published at

a time when the French mathematician was absorbed in developing the theory of automorphic functions. Moreover, these results appeared in the *American Journal* in the first years of its existence, that is, before it became recognized as a major mathematical publication. Such arguments, however, appear to be less convincing in the light of the following fact. In the first volume of the *American Journal* G.W. Hill's work on lunar motion was published, and this work, as Parshall and Rowe [1994, p. 93] state, "would later attract the attention of Henri Poincaré".

CONCLUSION

In the present article, we have considered several works of the second half of the 19th century, where, in our opinion, the beginnings of a new approach to the problem of solving Diophantine equations in rational numbers originated. This approach was connected with a considerable extension of the means for investigating these equations. Already in Sylvester's letter to Cayley of 23 October, 1856 [Parshall 1998, p. 93] and in [Sylvester 1858], we encounter a geometrical treatment of the problem of solving a third degree Diophantine equation, namely, as a problem of finding rational points on the corresponding curve. In [Lucas 1878], we find a clear geometrical formulation of the basic methods of finding rational points on a curve of third degree — the tangent, secant and conics methods — which was later repeated in [Lucas 1879]. In [Sylvester 1879/80], Sylvester points out that the conics method reduces to a combination of the first two methods and, apparently for the first time in the history of Diophantine analysis, he carries out a study of the structure of the set of rational solutions of a general third degree indeterminate equation, setting a plane elliptic curve. To be more exact, Sylvester considers the set of all rational points of a cubic generated by a single rational point by means of the tangent and secant methods. He introduces the notion of an index of a point from this set, and instead of operating with the coordinates of rational points, he turns to operations on their indices. Having established the rules for operating with indices, he obtains the first method for describing the structure of the stated set. His method, though, was rather cumbersome, since it involved a whole set of rules for operating with indices. To carry out his investigation, Sylvester used the results from the theory of algebraic curves. The American mathematician,

William Story, simplified Sylvester's theory of indices considerably, having somewhat changed their definition [Story 1880]. As a result, operations on indices were brought into line with operations on elliptic parameters of points. Thus, the structure of the set of rational points on a cubic could be described in terms of the parametrization of the cubic by means of elliptic functions. For his part, however, Story developed the theory of indices for its application to problems in the theory of algebraic curves and not for solving Diophantine equations. Therefore, he did not demand that the initial point and the coefficients of the cubic equation be rational.

Here, we have traced how the break occurred in the 19th century from the centuries-old tradition of the purely algebraic treatment of the problem of solving Diophantine equations in rational numbers. The picture presented here is, however, far from exhaustive. To consider the question of the transformation of Diophantine analysis at the beginning of the 20th century into algebraico-geometric terms, for example, it will be necessary to take into account the historical development of the algebraic geometry proper, and in particular of its methods and results that were applied to Diophantine analysis.

BIBLIOGRAPHY

- BASHMAKOVA (Isabella G.)
 [1968] Diophante et Fermat, *Revue d'histoire des sciences et de leurs applications*, 19 (1968), pp. 283–306.
 [1981] Arithmetic of Algebraic Curves from Diophantus to Poincaré, *Historia mathematica*, 8 (1981), pp. 393–416.
- CAUCHY (Augustin-Louis)
 [*Œuvres*] *Œuvres complètes*, 27 vols. (two series), Paris: Gauthier-Villars, 1882–1974.
 [1826] *Exercices de mathématiques*, Paris, 1826; *Œuvres* (II) 6, pp. 286–315.
- CLEBSCH (Rudolf Friedrich Alfred)
 [1864] Über einen Satz von Steiner und einige Punkte der Theorie der Curven dritter Ordnung, *Journal für die reine und angewandte Mathematik*, 63 (1864), pp. 94–121 .
- COOKE (Roger) & RICKEY (V. Frederick)
 [1989] W.E. Story of Hopkins and Clark, in Duren (Peter) *et al.*, eds., *A Century of Mathematics in America – Part III*, Providence: American Mathematical Society, 1989, pp. 29–76.
- DAHAN-DALMÉDICO (Amy) & PEIFFER (Jeanne)
 [1982] *Une histoire des mathématiques. Routes et dédales*, Paris: Études vivantes, 1982; 2^e éd., Paris: Éditions du Seuil, 1986, 314 p.
 [1986] *Routes et dédales* (Russian translation), Moscow: MIR, 1986.

- DESBOVES (Alain)
 [1879] Mémoire sur la résolution en nombres entiers de l'équation $aX^m + bY^m = cZ^n$, *Nouvelles annales de mathématiques*, 2^e série, 18 (1879), pp. 265–279, 398–410, 433–444, 481–499.
- DÉCAILLOT (Anne-Marie)
 [1998] L'arithméticien Édouard Lucas (1842–1891): théorie et instrumentation, *Revue d'histoire des mathématiques*, 4 (1998), pp. 191–236.
- DICKSON (Leonard Eugene)
 [1920] *History of the Theory of Numbers, vol. 2: Diophantine Analysis*, Washington: Carnegie Institute of Washington, 1920 (reprint. New York: Chelsea, 1952).
- DIEUDONNÉ (Jean), éd.
 [1978] *Abrégé d'histoire des mathématiques, 1700–1900*, t. I–II, Paris: Hermann, 1978.
- ELLISON (W. & F.)
 [1978] Théorie des nombres, [Abrégé], I, chap. V, pp. 165–334.
- EULER (Leonhard)
 [Opera] *Leonhardi Euleri Opera omnia*, ser. 1, 29 vol., Leipzig-Berlin: Teubner, 1911–1956.
 [1770] *Vollständige Anleitung zur Algebra, Zweyter Teil*, Petersbourg, 1770; *Opera* (I), 1, pp. 209–498.
- FERMAT (Pierre)
 [1670] *Doctrinae analyticae inventum novum* (compiled by J. de Billy from Fermat's letters); *Œuvres de Pierre Fermat*, t. 1, Paris: Blanchard, 1999, pp. 157–232.
- GOLDSTEIN (Catherine)
 [1995] *Un théorème de Fermat et ses lecteurs*, Saint-Denis: PUV, 1995.
- HARKIN (Duncan)
 [1957] On the Mathematical Work of François-Édouard-Anatole Lucas, *L'Enseignement mathématique*, 2^e série, 3 (1957), pp. 276–288.
- HOFMANN (Joseph Ehrenfried)
 [1961] Über zahlentheoretische Methoden Fermats und Eulers, ihre Zusammenhänge und ihre Bedeutung, *Archive for History of Exact Sciences*, 1 (1961), pp. 122–159.
- HURWITZ (Adolf)
 [1917] Über ternäre diophantische Gleichungen dritten Grades, *Vierteljahresschrift der Naturforschenden Gesellschaft in Zürich*, 62 (1917), pp. 207–229.
- JACOBI (Carl Gustav Jacob)
 [1835] De usu theoriae integralium ellipticorum et integralium abelianorum in analysi diophantea, *J. reine angew. Math.*, 13 (1835), pp. 353–355.
- KAUCHIKAS (Algerdas)
 [1979] *Diophantus and Indeterminate Analysis in the Works of European Mathematicians of the 13th–16th Centuries*, Dissertation, Moscow, 1979 (in Russian).
- LAGRANGE (Joseph Louis)
 [Œuvres] *Œuvres de Lagrange*, J.-A. Serret and G. Darboux, eds., 14 vol., Paris: Gauthiers-Villars, 1867–1892.
 [1777] Sur quelques problèmes de l'analyse de Diophante, *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin*, 1777; *Œuvres* 4, pp. 377–398.

LAVRINENKO (Tatiana A.)

- [1982] *Solving of Indeterminate Equations of Third and Forth Degrees in Rational Numbers in the 19th Century*, Moscow: deponir. VINITI AN SSSR, No. 3669–83, 1982 (in Russian).
- [1983] Solving of Indeterminate Equations of Third and Fourth Degrees in the Late Euler's Works, *Istoriko-Matematicheskie Issledovaniya*, 27 (1983), pp. 67–79 (in Russian).
- [1985] On Methods of Solving Indeterminate Equations in Rational Numbers in the 18th–19th centuries, *Istor.-Mat. Issledov.*, 28 (1985), pp. 202–223 (in Russian).
- [1988] Diophantine Equations in L. Euler's Works, in *The Development of Leonard Euler's Ideas and Modern Science*, Moscow: Nauka, 1988, pp. 153–165 (in Russian).

LUCAS (Édouard)

- [1873] *Recherches sur l'analyse indéterminée et l'arithmétique de Diophante*, Moulins: Desrosiers, 1873; reprint Paris: Blanchard, 1961.
- [1875] Questions d'analyse indéterminée, *Nouv. ann. math.*, 2^e série, 14 (1875), p. 526.
- [1877] Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'arithmétique supérieure, *Bulletino di bibliografia e di storia delle scienze matematiche e fisiche*, 10 (1877), pp. 129–193, 239–293.
- [1878] Sur l'analyse indéterminée du troisième degré et sur la question 802 (Sylvester), *Nouv. ann. math.*, 2^e série, 17 (1878), pp. 507–514.
- [1879] Sur l'analyse indéterminée du troisième degré. Démonstration de plusieurs théorèmes de M. Sylvester, *American Journal of Mathematics*, 2 (1879), pp. 178–185.

NEWTON (Isaac)

- [1971] *The Mathematical Papers of Isaac Newton*, vol. 4, ed. D.T. Whiteside, Cambridge, 1971.

PARSHALL (Karen Hunger) & ROWE (David E.)

- [1994] *The Emergence of the American Mathematical Research Community 1876–1900: J.J. Sylvester, Felix Klein, and E.H. Moore*, Providence: American Mathematical Society, 1994.

PARSHALL (Karen Hunger)

- [1998] *James Joseph Sylvester: Life and Work in Letters*, Oxford: Oxford University Press, 1998.

POINCARÉ (Jules Henri)

- [1901] Sur les propriétés arithmétiques des courbes algébriques, *Journal de mathématiques pures et appliquées*, 5^e série, 7 (1901), pp. 161–233.

RASHED (Roshdi), éd.

- [1984] Diophante, *Les Arithmétiques*, Paris: Les Belles Lettres, 1984 (introduction, notamment).

SALMON (George)

- [1879] *A Treatise on the Higher Plane Curves: Intended as a Sequel to a Treatise on Conic Sections*, 3d ed., Dublin, 1879.

SCHAPPACHER (Norbert)

- [1991] Développement de la loi de groupe sur une cubique, dans *Séminaire de théorie des nombres, Paris 1988/1989 (Progress in Mathematics 91)*, Boston: Birkhäuser, 1991, pp. 159–184.

SCHLESINGER (Ludwig)

- [1909] Über ein Problem der Diophantischen Analysis bei Fermat, Euler, Jacobi und Poincaré, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 17 (1909), pp. 57–67.

STORY (William E.)

- [1880] On the Theory of Rational Derivation on a Cubic Curve, *Amer. J. Math.*, 3 (1880), pp. 356–387.

SYLVESTER (James Joseph)

[*Mathematical Papers*] *Collected Mathematical Papers*, 4 vols., Cambridge: Cambridge University Press, 1904–1911.

- [1847a] An Account of a Discovery in the Theory of Numbers Relative to the Equation $Ax^3 + By^3 + Cz^3 = Dxyz$, *Philosophical Magazine*, 31 (1847), pp. 189–191; *Mathematical Papers*, 1, pp. 107–109.

- [1847b] On the Equation in Numbers $Ax^3 + By^3 + Cz^3 = Dxyz$ and Its Associate System of Equations, *Phil. Mag.*, 31 (1847), pp. 293–296; *Mathematical Papers*, 1, pp. 110–113.

- [1847c] On the General Solution (in Certain Cases) of the Equation $x^3 + y^3 + Az^3 = Mxyz$, etc., *Phil. Mag.*, 31 (1847), pp. 467–471; *Mathematical Papers*, 1, pp. 114–118.

- [1856] Recherches sur les solutions en nombres entiers positifs ou négatifs de l'équation cubique homogène à trois variables, *Annali di scienze matematiche e fisiche*, 7 (1856), pp. 398–400; *Mathematical Papers*, 2, pp. 63–64.

- [1858] Note on the Algebraical Theory of Derivative Points of Curves of the Third Degree, *Phil. Mag.*, 16 (1858), pp. 116–119; *Mathematical Papers*, 2, pp. 107–109.

- [1867] Question n° 802, *Nouv. ann. math.*, 2^e série, 6 (1867), p. 96.

- [1879/80] On Certain Ternary Cubic-Form Equations, *Amer. J. Math.*, 2 (1879), pp. 280–285 and 357–393; 3 (1880), pp. 58–88 and 179–189; *Mathematical Papers*, 3, pp. 312–391.

WEIL (André)

- [1983] *Number Theory. An Approach through History: from Hammurapi to Legendre*, Boston, etc.: Birkhäuser, 1983.