Historia Mathematica 8 (1981) 393-416

ARITHMETIC OF ALGEBRAIC CURVES FROM DIOPHANTUS TO POINCARÉ

BY ISABELLA G. BASHMAKOVA
DEPARTMENT OF MATHEMATICS,
MOSCOW STATE UNIVERSITY,
MOSCOW, USSR

SUMMARIES

This article contains an analysis of the methods for solving diophantine equations of second and third degrees in two unknowns, from the most ancient times to Poincaré. Special attention is paid to the works of Fermat, Euler, and Jacobi.

L'article contient l'analyse des méthodes diophantiennes pour résoudre les équations indéterminées du 2ème et 3ème degrés à deux inconnues de l'antiquité à Poincaré. Plus spécialement est étudié l'apport de Fermat, Euler, et Jacobi.

Статья содержит анализ методов решения неопределённых уравнений второй и третьей степени с двумя неизвестными от древности до Пуанкаре. Особое внимание уделяется вкладу Ферма, Эйлера и Якоби.

Algebraic geometry and Diophantine equations occupy principal positions in modern mathematics. Nowadays these subjects attract the minds of researchers just as powerfully as the theory of functions of a real variable and set theory excited scholars at the beginning of this century. It is generally known that Henri Poincaré's fundamental memoir [1901] served as a base for the unification of the two former disciplines. Indeed, Poincaré outlined a program for the construction of an extensive theory;

0315-0860/81/040393-24$02.00/0

he himself originated this theory while its further development was due to many outstanding mathematicians of our century, with André Weil holding the first place among all of them.

I shall discuss several ideas, methods, and achievements due to Poincaré. Note, however, that I do not by any means exhaust the treasures contained in his memoir:

> 1. In order to classify Diophantine equations Poincaré introduced a birational equivalence relation between corresponding homogeneous polynomials.
>
> 2. He constructed an arithmetic of plane algebraic curves of genus $g = 0$ and $g = 1$, and introduced, for the latter curves, addition of rational points. He also proved that with respect to this operation, the set of rational points of the curve constitutes an abelian group.
>
> 3. Poincaré formulated a hypothesis according to which the just-mentioned group possesses a finite number of generators.
>
> 4. For curves of genus $g > 1$ he discovered that, on the one hand, the introduction of a reasonable rule for the addition of rational points is impossible, but, on the other hand, that one might define the addition of "rational groups" consisting of g points each, i.e., the addition of classes of rational divisors.

As for terminology, the genus g of a plane algebraic curve is an integer equal to

$$(n - 1)(n - 2)/2 - d,$$

where n is the degree of the curve Γ, and d is the number of its double points. Curves of genus $g = 1$ are called *elliptic*. For $n = 3$ the corresponding curve Γ will be elliptic if and only if *it completely lacks singular points*.

Poincaré's ideas and methods as pointed out above have a long prehistory. It is my aim to consider some of the major issues as I see them.

In his *Arithmetic* [1893] Diophantus (middle of the third century A.D.) entirely solved in a purely algebraic way the problem concerning the rational points of second-degree curves. In the same work he used the tangent and secant methods (again treated in an algebraic way) for the discovery of rational points on curves of third degree. These are discussed at greater length below.

Even Zeuthen [1896] noted that Diophantus knew a general method for solving equations of the type

$$y^2 = ax^2 + bx + c \tag{1}$$

when either a or c was a perfect square. Diophantus' substitutions were

$$y = ax + m, \qquad y = kx + c,$$

respectively, with arbitrary parameters m and n.

In fact Diophantus actually knew much more. Let $f_2(x, y)$ be an irreducible polynomial of second degree in the field Q of rational numbers, and suppose that one rational solution of the equation

$$f_2(x, y) = 0 \tag{2}$$

is known. For this case Diophantus described a method of representing x and y by such rational functions $x = \phi(t)$, $y = \psi(t)$ such that $f_2[\phi(t), \psi(t)] \equiv 0$. Assuming various rational values for t, one might calculate all the solutions of Eq. (2).

Nowadays the corresponding proposition is formulated as follows: *a rational curve of second degree either does not contain any rational point at all; or, it is birationally equivalent to a straight line.* (For the sake of simplicity, the case in which the rational point is at the same time an infinite point is left aside. Diophantus treats this special case in a purely algebraic way.) [Bashmakova 1968].

This theorem is actually due to Diophantus, who proved it by stages using an algebraic approach. In Book II of the *Arithmetic* he offered a method for calculating a second rational solution for Eq. (2) when one of its solutions is known. Consider, for example, Diophantus' treatment of problem II_8 (or, for that matter, II_9) where it is required that the square a^2 be decomposed into a sum of two squares:

$$x^2 + y^2 = a^2, \qquad a^2 = 16. \tag{3}$$

Rational solutions of this equation are, e.g., $(0, a)$ and $(0, -a)$. In order to determine other solutions, Diophantus substitutes

$$y = kx - a. \tag{4}$$

Indeed, he says: "I form the square from any number of x minus as many units as there are in the side of 16, and let it be $2x - 4$." (For some reason the end of this passage is missing from the English translation of the *Arithmetic*.) Diophantus chooses 2 as one of the possible numbers while 4 is held fixed so that Eq. (4), with a fixed value of a, is an adequate letter formula of Diophantus' substitution.

The solution of Eq. (3) now leads to

$$(kx - a)^2 = a^2 - x^2,$$

so that

$$x = \frac{2ak}{k^2 + 1}, \quad y = a\,\frac{k^2 - 1}{k^2 + 1}.$$

Thus, x and y are represented by rational functions of the parameter k. Assuming $a^2 = 16$ and $k = 2$, Diophantus arrives at $x = 16/5$, $y = 12/5$, saying nothing, however, about the number of solutions, although this method makes it possible to calculate an infinity of them. He himself mentions this fact elsewhere (problem III_{19}): "We saw how to divide a square in an infinite number of ways."

Diophantus also knew how to treat a more general case than the one just described (and discussed previosuly by Zeuthen). Consider problem II_9, which might be reduced to the solution of the equation

$$x^2 + y^2 = N = a^2 + b^2, \tag{3'}$$

where $N = 13$. In order to find a rational solution of this equation Diophantus represents 13 as the sum of two squares, 4 and 9. Then, obviously, (3') possesses four rational solutions (2, 3), (2, -3), (-2, 3), and (-2, -3). Diophantus assumes

$$x = t + 2, \quad y = kt - 3, \tag{4'}$$

and, substituting these expressions in the initial equation, he arrives at

$$t = \frac{6k - 4}{k^2 + 1},$$

which means that x and y are now rational functions of t. Diophantus' solution corresponds to $k = 2$ but he adduces a remark to the effect that it is necessary to "take several x's, for example 2, and subtract 3." (Again, the English translation lacks this passage.)

In the subsequent exposition Diophantus repeatedly uses the same methods as those in problems II_8 and II_9, but only in two instances (lemmas to problems VI_{12} and VI_{15}) does he formulate his findings in a general way. Consider, for example, Problem VI_{12}, second lemma:

> *Given two numbers the sum of which is a square, an infinite number of squares can be found such that, when the square is multiplied by one of the given numbers and the product is added to the other, the result is a square.*

To put it another way, if

$$ax^2 + b = y^2, \quad a + b = \square ,$$

then the equation possesses an infinity of solutions.

What exactly does the restriction that the sum $a + b$ be a square mean? It is easy to see that, if $a + b = m^2$, the equation has a rational solution $(1, m)$. Diophantus proves this assertion by assuming

$$x = t + 1, \quad y = y$$

and arriving at an equation

$$at^2 + 2at + m^2 = y^2$$

whose free term is a perfect square. Therefore, other rational solutions of the equation might be determined in the usual way. By substituting $y = kt - m$, one has

$$t = 2\,\frac{a + km}{k^2 - a},$$

so that x and y are now rational functions of parameter k. One and only one solution of the problem corresponds to each value of this parameter.

Problem VI_{15}, lemma:

> *Given two numbers, if some square is multiplied into one of the numbers and the other number is subtracted from the product and the result is a square, then another square larger than the aforesaid square can always be found which has the same property.*

Therefore, if the equation

$$ax^2 - b = y^2$$

has a rational solution (p, q), it is possible to find another larger solution (p_1, q_1), and then yet another (p_2, q_2), etc., with $p < p_1 < p_2 < \cdots < p_n < \cdots$.

Diophantus proved this statement for $a = 3$, $b = 11$. In this instance $p = 2$, $q = 1$. After a substitution $x = t + p$, $y = y$, Diophantus arrived at

$$at^2 + 2apt + q^2 = y^2.$$

Assuming $y = q - kt$, one has

$$t = 2\,\frac{ap + kq}{k^2 - a}\,.$$

With $k^2 > a$, t is positive and $p_1 = t + p > p$.

Having symbols only for the designation of the unknowns and their first six powers, positive or negative, Diophantus only had to choose concrete numbers for his parameters to carry out the proof, and to calculate the solutions with these fixed parameters. This did not involve loss of generality either in reasoning or solution, because Diophantus did not use any special properties of the numbers he chose. The only exceptions were cases in which he had to apply pure number-theoretic analysis (for example, if the parameter should have been represented by a sum of two rational squares, etc.).

Note that Diophantus' methods admit a simple geometric interpretation. Suppose that Eq. (2) determines a curve L in a plane where the solution (x, y) is a point situated on the curve. If x and y are rational, the point is said to be *rational*.

It is not difficult to see now that each of Diophantus' substitutions (for example, (4) or (4')) is equivalent to the construction of a pencil of straight lines passing through a rational point $A(x_0, y_0)$ situated on the curve L and having a rational slope k. Each straight line of the pencil will intersect the curve L in one more rational point.

In Book IV of the *Arithmetic* Diophantus considered problems requiring indeterminate equations of third, fourth, and sixth degrees for their solution. At first, these equations determined curves of genus 0, so that he was able to represent the unknowns as rational functions of the parameter. But in subsequent problems the first curves of genus 1 made their appearance, and for such curves the representation just mentioned is impossible. How did Diophantus manage to solve the corresponding equations for these problems?

First, it is helpful to recall modern methods used to determine rational points on elliptic curves. Let the curve L be given by the equation

$$F_3(x, y) = 0, \tag{5}$$

where $F_3(x, y)$ is a polynomial of third degree, irreducible in Q. Suppose also that two rational points, $A(x_1, y_1)$ and $B(x_2, y_2)$ exist on curve L.

The first method (the *secant method*, as I shall call it) of calculating other rational points consists in constructing a straight line passing through A and B. This line will intersect curve L (of third degree) in one more point and it is easily seen that the latter will be rational.

The second method (the *tangent method*) is applied when only one rational point $A(x_1, y_1)$ is known. In essence, it amounts to drawing a tangent which passes through point A:

$$y - y_1 = k(x - x_1), \quad k = \frac{dy}{dx} = - \frac{\partial F_3/\partial x}{\partial F_3/\partial y}(x_1, y_1).$$

The point of tangency is a double point and the tangent will intersect curve L only in one more point which again will be rational.

Diophantus anticipated both these methods. He used the tangent method for the solution of problems IV_{24} and VI_{18}. In the former case he considered the equation

$$x(a - x) = y^3 - y, \qquad (6)$$

where $a = 6$. Its obvious rational solutions are (0, 1) and (0, -1). Diophantus chooses the second solution and substitutes

$$y = kx - 1. \qquad (7)$$

He begins by assuming $k = 2$, but his analysis proved that k cannot be taken arbitrarily. Its value must be such as to assure that x vanishes from the subsequent equation. Thus, Diophantus arrived at $k = a/2$. It is not difficult to see that with such k the straight line (7) is tangent to curve (6). This procedure for the determination of k is equivalent to a purely algebraic calculation of the derivative dy/dx of the implicit function (6) at the point (0, -1) [Bashmakova 1968].

In problem VI_{18} Diophantus encounters the equation

$$x^3 - 3x^2 + 3x + 1 = y^2, \qquad (8)$$

which possesses a rational solution (0, 1). He determines another rational solution by means of a substitution

$$y = (3/2)x + 1. \qquad (9)$$

This time he chooses a value of k ($k = 3/2$) which immediately causes x to vanish from the subsequent equation. Again, his choice means that the corresponding straight line (9) from the pencil of lines (7) touches curve (8) (at the point (0, 1)).

Referring to his *Porisms* (a work which has been lost), Diophantus also claimed that he had found the rational solutions of the equation $x^3 + y^3 = a^3 - b^3$ for any values of a and b. I shall return to this problem in the following section.

Diophantus applied the secant method for the solution of problems IV_{26} and IV_{27}. In both these instances one of the two given rational points was finite and the other infinite. Thus, in the former problem Diophantus arrived at an equation

$$8x^3 + x^2 - 8x - 1 = y^3 \qquad (10)$$

which has a finite rational solution (0, -1). He substituted

$$y = 2x - 1 \tag{11}$$

and determined $x = 14/13$, $y = 15/13$.

What, now, is the geometric meaning of this substitution? Why does the straight line (11) come into contact with the curve of third degree (10) only in one point? Indeed, this straight line is not tangent to the curve at the point (0, -1)! The answer is simple: the curve (10) and the straight line (11) possess a common infinite rational point.

Diophantus solves problem IV_{27} in the same way [Bashmakova 1968].

Last, equations of the type

$$y^2 = Ax^4 + Bx^3 + Cx^2 + Dx + E,$$

with $A = \alpha^2$ and $E = \gamma^2$ appear in problems IV_{28} and VI_{10}. In each of these instances Diophantus uses the same substitution, $y = \alpha x^2 + \beta x + \gamma$, choosing a value of β which causes all the terms of the subsequent equation except those containing x^2 and x^3 to vanish. I do not trace the further history of this method and I shall not discuss its geometric meaning.

The examples offered above seem to testify that Diophantus came to understand that, generally speaking, it is not possible to represent the unknowns x and y of indeterminate equations of third degree as rational functions of a parameter. At least, he did not try to find such representations but offered instead a method for determining one more rational solution of the equation given one or two such solutions.

The situation here is similar to that which arose in antiquity with respect to duplicating the cube and squaring the circle. Beginning at least with Euclid, mathematicians were convinced that these problems did not admit a graphical solution by means of ruler and compass; they did not try to find such solutions, but, at the same time, they were unable to prove the insolubility of such problems.

In the 16th century, European scholars rediscovered Diophantus' *Arithmetic*. Xylander (Wilhelm Holzmann) was the first to translate it into Latin. His translation appeared in 1575. Three years before this, R. Bombelli included 143 problems from the *Arithmetic* in his celebrated *Algebra*.

It is remarkable that, on the one hand, *before* the publication of Xylander's translation not a single European mathematician thought of applying the doctrine of indeterminate equations to the solution of problems in Diophantine analysis. Such problems were solved in a purely arithmetical manner. On the other hand, once having acquainted themselves with the *Arithmetic*, mathematicians soon grasped Diophantus' methods.

Using such methods, Bombelli introduced negative and complex numbers. He thoroughly understood Diophantus' method of solving indeterminate equations of the type $f_2(x, y) = 0$, although mathematicians of the Arab East preceded Bombelli in this respect. Bombelli also paid due attention to the tangent method. He was the first to apply this method to the solution of

$$x^3 + y^3 = a^3 - b^3, \tag{12}$$

with $a = 4$ and $b = 3$ (i.e., with the same values of these parameters as those used by Diophantus).

In his *Zetetica*, F. Viète (1540-1603) employed his new letter-calculus for the solution of Diophantine problems. In actual fact, he thereby imparted a modern algebraic appearance to them. He also solved Eq. (12) in the general case, though with the additional restriction that $a^3 > 2b^3$.

Only Pierre Fermat (1601-1665), the founder of the theory of numbers and the modern doctrine of indeterminate equations, had been able to force his way to the innermost layers of Diophantus' *Arithmetic*. It is generally known that he introduced the so-called method of infinite descent, one of the most powerful methods used in the theory of numbers. It is less well known that Fermat made a decisive step forward by showing that the calculations of Diophantus' secant and tangent methods might be repeated consecutively so as to provide an infinity of rational solutions for equations which determine elliptic curves. In his remarks on the *Arithmetic*, Fermat called these iterations "ma méthode" and "la méthode que je inventée" [Fermat 1670a, Observations N37, 38, 39].

J. de Billy explicated Fermat's method in more detail. In the introduction to his *Inventum novum*, compiled from Fermat's letters, de Billy wrote:

> *...qui jamais a donné autant de solutions que l'on veut pour les expressions composées de cinq termes de degrés successifs [i.e., for equations of the type $y^2 = ax^4 + bx^3 + cx^2 + dx + e$]? Qui, des racines primitives, à su en tirer de dérivées du premier ordre, du second, du troisième, et ainsi de suite indéfiniment? Personne sans doute; à Fermat seul appartient cette découverte*. [Fermat 1670b, 326]

De Billy's statement is also completely valid for equations of the type $f_3(x, y) = 0$. Fermat's *méthode* may be illustrated by his own remark XI on the *Arithmetic*:

> *Si l'on cherche* deux bicarrées dont la différence soit égale à celle de leurs racines, *on pourra résoudre la question en employant l'artifice de ma méthode. Qu'on cherche, en effet, deux bicarrées dont la différence soit un cube, et tels que la différence de leurs racines soit* 1. *On trouvera, par la première opération, les racines* -9/22 *et* 13/22. *Le premier de ces deux nombres étant affecté du signe -, on réitérera l'opération suivant ma méthode en égalant la première racine à x* - 9/22, *la seconde à x* + 13/22, *et l'on obtiendra ainsi des nombres positifs satisfaisant au problème.* [Fermat 1670, 248-249]

Thus, Fermat solves the equation

$$y^4 - x^4 = z^3. \tag{*}$$

He assumes $y - x = 1$ or $y = x + 1$, so that the equation changes to

$$4x^3 + 6x^2 + 4x + 1 = z^3. \tag{13}$$

The left-hand side is an irreducible polynomial of third degree, and its free term is a cube. Its obvious rational solu tion is (0, 1), and it is possible to find a second solution by means of Diophantus' tangent method. Assume

$$z = (4/3)x + 1, \tag{14}$$

which is what Fermat called "la première opération" [Fermat 1670a]. The calculations lead to

$$x_1 = -9/22, \quad y_1 = x_1 + 1 = 13/22, \quad z_1 = 5/11.$$

Now $x_1 < 0$, whereas Fermat restricts himself to solutions belonging to Q^+. This means that (-9/22, 13/22, 5/11) is not a solution of Eq. (*). In order to find a positive solution

Fermat suggests that the operation be repeated ("réitérera l'opération") and puts $x = t - 9/22$, i.e., "shifts" the curve (L) determined by Eq. (13). What exactly is achieved by this "shift"?

From a modern point of view, a repetition of the operation is a construction of a tangent to curve L at the point $M_1(-9/22, 5/11)$ or, otherwise, a substitution

$$z = k_1(x + 9/22) + 5/11, \tag{15}$$

where k_1 is the slope of the tangent at the point M_1.

However, Fermat (like, of course, Diophantus) reasoned in terms of algebra [1]. First and foremost, he wanted to transform Eq. (10) to a new equation of the type $y^3 = a^3x^3 + bx^2 + cx + d$, with a cube as its free term. Fermat achieved this goal by means of the "shift" mentioned above, $x = t - 9/22$, after which his equation (10) became

$$4t^3 + At^2 + Bt + z_1^3 = z^3, \tag{13'}$$

where $z_1 = 5/11$. A second substitution of the type of (14),

$$z = \frac{B}{3z_1^2} t + z_1, \tag{14'}$$

is now possible. This permits one to determine the solution (t_2, z_2) and therefore, the triplet (x_2, y_2, z_2). Note that in similar cases Euler proceeded in exactly the same way [Euler 1770, Section 2, §§120 and 153].

Fermat's *méthode* thus represents a regular procedure for a reiterated application of the tangent method. It furnishes the "primitive solution" and "derivative solutions." And Fermat also employed a quite similar method for determining rational solutions of the equations

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

and

$$a_1x^2 + b_1x + c_1 = y^2,$$
$$a_2x^2 + b_2x + c_2 = z^2.$$

Therefore he was the first to formulate the problem of calculating an infinity of rational points on elliptic curves, and to offer a method for determining them.

Three final remarks:

1. Fermat knew that the reiteration of the tangent method did not provide an infinity of solutions in all cases. In other words, he knew that elliptic curves might contain points of a finite order. The following examples are to be found in the *Inventum novum:*

> *solutions* (0, 1) *and* (0, -1) *for the equation* $y^3 = x^3 + 1$; *the solution* (-1, 1) *for the equation* $y^3 = x^3 + 2$.

Euler adduced similar examples in his *Vollständige Anleitung* [1770].

2. Fermat showed that Diophantus' statement on the solvability of Eq. (12) might be proved by means of a reiterated version of the tangent method (see [Hofmann 1961]).

3. Diophantus knew that the difference of two cubes could always be represented as a sum of two other cubes, and he claimed to have proved this proposition. This fact is circumstantial evidence of Diophantus' ability to apply the tangent method repeatedly.

Euler introduced essentially new ideas into Diophantine analysis. Of course, the exposition given here is restricted to a description of his works pertaining to the determination of rational points on elliptic curves.

Euler [1770] systematized and developed all previous research concerning curves

$$y^2 = f_3(x), \quad y^2 = f_4(x), \quad y^3 = f_3(x),$$

where $f_n(x)$ is a polynomial of nth degree with integral rational coefficients. He determined rational points on these curves by means of the tangent method and he applied the secant method in the same instances as Diophantus, i.e., when one of the given rational points of the elliptic curve was infinite.

Unlike his predecessors, Euler precisely showed the difference between the calculations of rational solutions for indeterminate equations of second and third degrees. He wrote

> *Zum voraus ist auch hier* [*i.e., for equations of third degree*] *dieses zu merken, daß man keine allgemeine Auflösung geben kann, wie eben geschehen, sondern eine*

> *jede Operation giebt uns nur einen einzigen Werth für x zu erkennen, da hingegen die obengebrauchte Methode auf einmahl zu unendlich viel Auflösungen leitet.*
> [Euler 1770, Section 2, §112]

Besides this, Euler discovered the condition which ensured that all the rational solutions of the equation

$$y^2 = ax^3 + bx^2 + cx + d$$

might be represented by rational functions of a parameter. He noted that the polynomial on the right-hand side should possess a double root:

$$ax^3 + bx^2 + cx + d = a(x - \alpha)^2(x - \beta).$$

It turns out that Euler's condition is not only sufficient but also necessary. However, given his level of knowledge in the field of algebraic curves, it was impossible for him to discover this fact.

Late in life Euler resumed his study of the subject and, for the first time ever, applied the secant method to the case in which two terminal rational points of an elliptic curve were known. This research was published posthumously, and has been analyzed by Hofmann [1961].

Euler also commenced a study in a completely different direction. His work seemed to have nothing in common with Diophantine analysis, but it subsequently threw unexpected light on such problems.

Generally it is thought that only Poincaré noticed the connection between Diophantine analysis and the addition theorem for elliptic integrals. Actually, this is not the case, as Jacobi published a short note, "On the Application of the Theory of Elliptic Integrals and Abelian Integrals to Diophantine Analysis" [1835].

Jacobi formulated the problems of indeterminate analysis studied by Euler in his posthumously published memoirs in the following way:

Dato numero rationali x, qui expressionem

$$(a + bx + cx^2 + dx^3 + ex^4)^{1/2}$$

et ipsam rationalem reddit, alios eiusmodi innumeros valores ipsius x detegendi.

Given, a rational number x, which makes the expression

$$(a + bx + cx^2 + dx^3 + ex^4)^{1/2}$$

rational; to find, an infinity of other values of x of the same kind. [Jacobi 1835, 53]

[Note: For technical reasons throughout this article the exponent $^{1/2}$ has been used rather than the radical symbol i.e., $a^{1/2}$ instead of $\sqrt{a}$. The original Latin, of course, used the radical notation.]

Jacobi went on to state that Euler's method of analyzing these problems coincided exactly with the procedure used to discover the addition theorem for elliptic integrals. Although Euler did not point out the coincidence, Jacobi believed that Euler could hardly have failed to notice it.

In order to explain the connection between Diophantine analysis and the addition theorem, Jacobi adduced the theorems due to Euler. Denoting

$$f(x) = a + bx + cx^2 + dx^3 + ex^4$$

and

$$\Pi(x) = \int_0^x \frac{dx}{(f(x))^{1/2}},$$

he formulated Euler's theorems in the following ways:

I. Proposita aequatione transcendenti

$$\Pi(z) = \Pi(x) + \Pi(y),$$

simul et ipsum z et ipsum $f(z)^{1/2}$ rationaliter *exhiberi per* x, y, $(f(x))^{1/2}$, $(f(y))^{1/2}$.

I. If a transcendental equation

$$\Pi(z) = \Pi(x) + \Pi(y),$$

is given, then z and $(f(z))^{1/2}$ might be simultaneously represented by rational *functions of x, y, $(f(x))^{1/2}$, and $(f(y))^{1/2}$.* [Jacobi 1835, 53]

II. Proposita aequatione

$$\Pi(y) = n \Pi(x).$$

ubi n numeros integer, simul et ipsum y et ispum $(f(y))^{1/2}$ per x, $(f(x))^{1/2}$ rationaliter *exhiberi.*

II. If an equation

$$\Pi(y) = n \Pi(x).$$

is given with n an integer, than y and $(f(y))^{1/2}$ might be simultaneously represented by rational *functions of x and $(f(x))^{1/2}$.* [Jacobi 1835, 54]

III. Proposita aequatione

$$\Pi(x) = m_1 \Pi(x_1) + m_2 \Pi(x_2) + \cdots + m_n \Pi(x_n),$$

ubi m_1, m_2, ..., m_n sunt numeri integri quilibit positivi vel negativi, simul et ipsum x et radicale $(f(x))^{1/2}$ per x_1, x_2, ..., x_n et radicale $(f(x_1))^{1/2}$, $(f(x_2))^{1/2}$, ..., $(f(x_n))^{1/2}$ rationaliter exprimi.

III. If an equation

$$\Pi(x) = m_1 \Pi(x_1) + m_2 \Pi(x_2) + \cdots + m_n \Pi(x_n),$$

is given with m_1, m_2, ..., m_n any integers, positive or negative, then x and $(f(x))^{1/2}$ might be simultaneously represented by rational *functions of x_1, x_2, ..., x_n and radicals $(f(x_1))^{1/2}$, $(f(x_2))^{1/2}$, ..., $(f(x_n))^{1/2}$.* [Jacobi 1835, 54]

Consider, for example, a general case of theorem II. Suppose a rational value of x is given which causes $(f(x))^{1/2}$ to be rational. Then, Jacobi noted, by means of a multiple elliptic integral it is possible to determine an infinity of such rational values of y for which $(f(y))^{1/2}$ will also become rational. These values of y will satisfy a transcendental equation

$$\Pi(y) = n \ \Pi(x).$$

Euler's analysis then makes it possible to calculate the desired solutions of this equation. To put it another way, given a rational point $(x, (f(x))^{1/2})$, Theorem II provides the means for determining in general an infinity of other rational points of an elliptic curve $y^2 = f(x)$.

Jacobi next turned his attention to Theorem III. This theorem claims that, given two rational values x_1 and x_2 such that $(f(x_1))^{1/2}$ and $(f(x_2))^{1/2}$ are also rational, Euler's methods enable one to calculate an infinity of other values of x which also satisfy the same condition. These values are solutions of equations

$$\Pi(x) = m_1 \ \Pi(x_1) + m_2 \ \Pi(x_2),$$

where m_1 and m_2 are any integers.

Thus, Jacobi discovered the connection between problems of Diophantine analysis for elliptic curves and Euler's addition theorems.

Nowadays it would be natural to say that the point $(z, (f(z))^{1/2})$, a solution of a transcendental equation $\Pi(z) = \Pi(x) + \Pi(y)$, is a "sum" of points $(x, (f(x))^{1/2})$ and $(y, (f(y))^{1/2})$, while the point $(u, (f(u))^{1/2})$, a solution of the equation $\Pi(u) = n\Pi(x)$, is a point with multiplicity n, $(x, (f(x))^{1/2})$. In this language, the theorems Jacobi formulated would have meant that the set of rational points of an elliptic curve constitutes a module over a ring of integers. However, neither Jacobi nor his contemporaries were inclined to apply arithmetical operations to points or any other objects likewise alien to classical arithmetic. More than half a century had to pass before mathematicians learned to make such applications and became used to them.

Although Jacobi did not explicitly introduce the "addition" of points of an elliptic curve, in essence he profoundly studied the structure of the set of such points. Indeed, he asked himself whether or not Theorem II always enabled one to calculate an infinity of rational points from one given rational point. As Jacobi put it,

> *Exeptionum casus proveniunt, si pro dato valore a fit* $\Pi(a)$ *pars aliquota indicis.*
>
> *Exceptional cases appear when, for a given value of a,* $\Pi(a)$ *would be an aliquot part of the index.* [Jacobi 1935, 55. The index is Jacobi's term for the period of the elliptic integral.]

In such instances, Jacobi continued, only a finite number of noncoincident rational points were determined. Basically he discovered that, in the general case, the rational points constitute a module with a torsion. Jacobi ended his note with certain generalizations this time striving to ascertain the connection between Diophantine analysis and the abelian addition theorem.

If we now consider curves of genus $g \geq 2$ rather than elliptic curves, it is impossible to introduce any reasonable procedure for the addition of their points (i.e., an addition which would cause the set of rational points to constitute a module). Poincaré pointed out this fact in his famous memoir:

> *Il n'est plus vrai que de la connaissance d'un point rationnel on puisse déduire celle d'une infinité d'autres points rationnels. Mais de la connaissance d'un* groupe *rationnel (et par conséquent de celle d'un point rationnel) on peut déduire celle d'une infinité d'autres groupes rationnels.* [Poincaré 1901, 231]

According to Poincaré, a "rational group" is a system of points of an algebraic curve such that any symmetric function of their coordinates must be rational. A modern term is "rational divisor" rather than "rational group."

In the 1920s A. Weil developed Poincaré's idea. He showed that propositions valid for a set of rational points of an elliptic curve also hold for any abelian manifolds. Jacobian manifolds, directly connected with the curve, present the most important case of such manifolds. In essence, at the end of his note Jacobi himself considered exactly these manifolds.

If Abel's theorem rather than Euler's proposition is applied to Diophantine analysis, then the following statement is easily deduced, as Jacobi noted:

> *Designante $f(x)$ functionem ipsius x rationalem integram quinti aut sexti ordinis, si datur unus valor ipsius x rationalis, pro quo etiam $(f(x))^{1/2}$ rationale fiat, dantur innumeri ipsius x valores formae $a + bc^{1/2}$, in qua a, b, c quantitates rationales, pro quibus etiam $(f(x))^{1/2}$ eandem formam induit $a' + b'c^{1/2}$, ubi rursus a', b' rationales.*
>
> *Let $f(x)$ denote an integral rational function of x of fifth or sixth degree; if some rational value of x*

> *is given such that $(f(x))^{1/2}$ is also rational, then an infinity of values of x of the form $a + bc^{1/2}$ with a, b, c rational quantities is also given, and for these values of x $(f(x))^{1/2}$ assumes the same form, $a' + b'c^{1/2}$, with rational a' and b'.* [Jacobi 1835, 55]

Thus Jacobi considered hyperelliptic curves

$$y^2 = f_5(x) \quad \text{and} \quad y^2 = f_6(x)$$

of genus 2. Referring to the corresponding case of Abel's addition theorem, Jacobi concluded that if one rational point (x, y) was given, it was possible to determine two points, (x_1, y_1) and (x_2, y_2), whose abscissas satisfy an equation of second degree with rational coefficients, i.e., $x_1 + x_2 = m$, $x_1x_2 = l$, where m and l are rational. Therefore, $x_1 = a + bc^{1/2}$, $x_2 = a - bc^{1/2}$. The ordinates of the two points are also conjugate and belong to the same field $Q(c^{1/2})$. Using the terminology due to Poincaré, one might say that the two points constitute a rational group of two elements. Thus, Jacobi in essence turned from the addition of points to the addition of "rational groups" of points, or divisors. This is the substance of his idea.

Jacobi then discussed a more general case. He wrote:

> *Designante $f(x)$ functionem ipsius x rationalem integram $(2n + 1)^{ti}$ aut $(2n + 2)^{ti}$ ordinis, si datur valor ipsius x rationalis, pro quo etiam $(f(x))^{1/2}$ rationale fiat, dantur innumerae aequationes n^{ti} gradus, quarum coefficientes numeri rationales sunt, ita comparatae, ut designante x earum radicem quamlibet, radicale $(f(x))^{1/2}$ per ipsam radicem x et numeros rationales rationaliter exhiberi queat.*
>
> *Let $f(x)$ denote an integral rational function of degree $(2n + 1)$ or $(2n + 2)$; if a rational value of x is given which leads to a rational $(f(x))^{1/2}$, then an infinity of equations of nth degree with rational coefficients is given; likewise, if x is any of their roots, then the radical $(f(x))^{1/2}$ might be represented as a rational function of x and* [some] *rational numbers.* [Jacobi 1835, 55]

Here Jacobi considered hyperelliptic curves of genus n. For this case Abel's theorem makes it possible to study, instead of one rational point, "rational groups" of n points, i.e., groups of points for which any symmetric function is rational.

Each ordinate is represented by a rational function of the corresponding abscissa so that it is sufficient to know only the abscissas of the points. As quoted above, Jacobi himself formulated the condition for the *n* points to constitute a "rational group" somewhat differently; according to him, the abscissas of these points must satisfy an algebraic equation of *n*th degree with rational coefficients.

Last, Jacobi considered a still more general case in which y is not equal to $(f(x))^{1/2}$ but is represented by an algebraic equation $f_n(x, y) = 0$, where $f_n(x, y)$ is a polynomial with rational coefficients. It would have been necessary to refer to Abel's theorem for integrals of arbitrary algebraic functions. However, Jacobi did not go into detail. He only expressed his hope that mathematicians would be able to derive benefits for indeterminate analysis from integral calculus similar to those he had obtained from Euler's doctrine of elliptic functions for the problems of Diophantine analysis. His words proved to be prophetic.

Jacobi was the first to turn from algebraic to analytical treatment of the problems of Diophantine analysis, and he connected these problems with the addition theorem for elliptic integrals. He also outlined a plan for constructing a similar theory for curves of higher degrees; basically, he considered rational groups of points and defined the addition of such groups by means of Abel's theorem. This means that Jacobi actually generalized the achievements relating to elliptic curves to include what today are known as arbitrary Jacobian manifolds.

It seems that Jacobi's contemporaries did not take note of this work by Jacobi on algebraic curves. Poincaré, who constructed the arithmetic of algebraic curves anew, did not know it either.

In the period following 1835 mathematicians came to study algebraic curves with greater insight. Even B. Riemann classified equations $f(x, y) = 0$ ($f(x, y)$ a polynomial with complex coefficients) assuming birational transformations as his basis. He thus discovered their most important invariant, the genus of the curve. A. Clebsch and other scholars of the second half of the last century algebraicized Riemann's methods, thereby establishing the origins of the algebraic geometry of curves. Still, Poincaré was the first to study the arithmetic of algebraic curves.

In 1901 Poincaré set forth his main ideas in a memoir which offered, as he put it in the introduction: "plutôt un programme d'étude qu'une véritable théorie" [Poincaré 1901, 161]. In order to systematize a large number of problems in Diophantine analysis, Poincaré devised a new classification of homogeneous polynomials of higher degrees, a classification similar to the one which Gauss adopted for quadratic forms. He defined curves by homogeneous coordinates and called two curves equivalent, or belonging to the same class, if they might be changed one into the other by means of a birational transformation. He conducted his research using the field of rational numbers. As compared with Jacobi, the introduction of a birational classification was a new step in the right direction.

Poincaré then considered rational curves of genus 0. He proved his well-known theorem about curves of this genus, namely, that any such curve of degree m ($m > 2$) is birationally equivalent to a curve of degree ($m - 2$). It followed that any such curve was birationally equivalent either to a conic section (if $m = 2k$), or to a straight line (if $m = 2k + 1$). However, Hilbert and Hurwitz [1890] proved this statement ten years earlier, a fact of which, again, Poincaré was unaware. Thus, for curves of genus 0 the study of the structure of the set of its rational points was reduced to the examination of the rational points of a conic section, a problem whose solution is due to Diophantus.

Poincaré devoted the main part of his memoir to elliptic curves. Like Jacobi, he based his work on Euler's addition theorem. But Poincaré studied his subject more carefully than Jacobi, in accordance with the contemporary demands for mathematical rigor. Moreover, Poincaré discovered the connection between Diophantus' tangent and secant methods on the one hand and Euler's addition theorems I and II on the other. Also, whereas Jacobi, like Euler before him, restricted himslef to a purely analytic explication without resorting to geometric interpretation, Poincaré, throughout his memoir, spoke about elliptic arguments of points (that is, about the points of the parallelogram of periods which correspond to the points of the elliptic curve), and about their addition and multiplication by a number rather than about integrals. He used geometric language again and again.

Poincaré defined the rank of an elliptic curve as the least number of rational points from which all the rest are derived by means of rational operations. Like the genus, the rank is an invariant of birational transformations.

Concerning this new notion, Poincaré formulated the following fundamental question:

> *Quelles valeurs peut-on attribuer au nombre entier que nous avons appelé le rang d'une cubique rationelle?*
> [Poincaré 1901, 173]

One might thus infer that Poincaré thought that the rank is finite. This indirectly expressed statement was subsequently called Poincaré's hypothesis. Mordell [1922] proved it by means of the method of descent.

As to the particular question about the rank of a cubic, the answer is unknown even today. On the one hand, it is not even known whether or not the rank is bounded, although, on the other hand, not a single curve with a rank exceeding 11 is known.

Poincaré also studied curves of genus 1. He deduced a condition for the equivalence of two such curves of degrees *m* and *p* ($m > p$), respectively. It turned out that a necessary and sufficient condition for equivalence required that the curve of degree *m* possess a rational group of *p* points. It followed that if there were *one* rational point on the curve of degree *m*, a point which could be assumed to constitute a rational group of three points merged into one, this curve would be birationally equivalent to a cubic.

This, then, is Poincaré's main achievement concerning curves of genus 1. As to elliptic curves of third degree, all the known methods for the determination of their rational points go back to Diophantus.

Poincaré concluded his memoir by suggesting two possible methods for subsequent generalization. One was the study of curves considered in an algebraic extension of the domain of rationality; the other involved the study of curves with genus larger than 1. In order to treat the latter case he developed in more detail his concept of a rational group of points, a concept which superseded the idea of a rational point for curves of higher degrees.

By the end of the 1920s Weil undertook both approaches. He proved the theorem on the finiteness of the rank for curves of any genus and in any field. It goes without saying that Weil applied addition of "rational groups," or divisors, rather than points [Weil 1929].

Diophantus' studies, continued by such eminent mathematicians as Fermat, Euler, Jacobi, and Poincaré, retain their interest even today. Jacobi changed Diophantus' purely algebraic methods for analytic ones. Poincaré's memoir was the beginning of a synthesis of the algebraic, analytic, and geometrical directions. Nowadays we are witnessing the realization of this synthesis by means of modern commutative algebra, this being, in a sense, a return to Diophantus' original point of view.

ACKNOWLEDGMENT

This article is a somewhat revised version of [Bashmakova 1975], published in Russian. O. B. Sheynin translated the Russian text.

NOTE

[1] D. T. Whiteside has recently published Newton's mathematical papers. These clearly show that Newton devoted much attention to, and attained important achievements in, Diophantine analysis. It should be emphasized that it was Newton who offered the first geometric interpretation of the methods for calculating rational solutions of indeterminate equations of second and third degrees. (See [Newton 1971].)

REFERENCES

Bashmakova, I. G. 1968. Diophante et Fermat. *Revue d'histoire des sciences et de leurs applications* 19, 283-306. Original Russian version in *Istoriko-mathematicheskie issledovania* 17 (1966).

——— 1975. Arithmetic of algebraic curves (from Diophantus to Poincaré). *Istoriko-mathematicheskie issledovania* 20, 104-124. [in Russian]

Diophantus. 1893. *Diophanti Alexandrini, arithmetica* (Bilingual Greek-Latin edition). *Opera omnia* 1, P. Tannery, ed. Leipzig. English translation in T. L. Heath, *Diophantus of Alexandria,* pp. 129-246. Cambridge, England, 1910.

Euler, L. 1770. Vollständige Anleitung zur Algebra. *Opera omnia* 1 (1), 209-498. Leipzig and Berlin.

Fermat, P. 1670a. Observations sur Diophante. *Oeuvres* 3, 241-276. Paris. This work was first published posthumously.

——— 1670b. Inventum novum (compiled by J. de Billy from Fermat's letters). *Oeuvres* 3, 325-400. Paris.

Hilbert, D., & Hurwitz, A., 1890. Über die diophantischen Gleichungen vom Geschlecht Null. *Acta Mathematica* 14, 217-224.

Hofmann, J. E. 1961. Über zahlentheoretische Methoden Fermats und Eulers, ... *Archive for History of Exact Sciences* 1 (2), 122-159.

Jacobi, C. G. J. 1835. De usu theoriae integralium ellipticorum et integralium abelianorum in analysi Diophantea. *Journal für die reine und angewandte Mathematik* 13, 353-355. Reprinted in C. G. J. Jacobi, *Gesammelte Werke* 2, 53-55. Berlin, 1882.

Mordell, L. J. 1922. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proceedings of the Cambridge Philosophical Society* 21, 179-192.

Newton, I. 1971. *Mathematical papers,* D. T. Whiteside, ed., Vol. 4. Cambridge, England.

Poincaré, H. 1901. Sur les propriétés arithmétiques des courbes algébraiques. *Journal des mathématiques pures et appliquées, Series V, 7, 161-233.*

Weil, A. 1921. L'arithmétique sur les courbes algébraiques. *Acta Mathematica,* 52, 281-315.

Zeuthen, H. G. 1896. *Geschichte der Mathematik im Altertum und Mittelalter.* Kopenhagen.