DIOPHANTUS OF ALEXANDRIA

A STUDY IN THE HISTORY OF GREEK ALGEBRA

BY

SIR THOMAS L. HEATH, K.C.B.,

SC.D., SOMETIME FELLOW OF TRINITY COLLEGE, CAMBRIDGE

SECOND EDITION

WITH A SUPPLEMENT CONTAINING AN ACCOUNT OF FERMAT'S THEOREMS AND PROBLEMS CONNECTED WITH DIOPHANTINE ANALYSIS AND SOME SOLUTIONS OF DIOPHANTINE PROBLEMS BY EULER

Cambridge:
at the University Press
1910

The Indian Solution.

If the Greeks did not accomplish the general solution of our equation, it is all the more extraordinary that we should have such a general solution in practical use among the Indians as early as the time of Brahmagupta (born 598 A.D.) under the name of the "cyclic method." Whether this method was evolved by the Indians themselves, or was due to Greek influence and inspiration, is disputed. Hankel held the former view[1]; Tannery held the latter and showed how, from the Greek manner of deducing from one approximation to a surd a nearer approximation, it is possible, by simple steps, to pass to the Indian method[2]. The question presumably cannot be finally decided unless by the discovery of fresh documents; but, so far as the other cases of solution of indeterminate equations by the Indians help to suggest a presumption on the subject, they are, I think, rather in favour of the hypothesis of ultimate Greek origin. Thus the solution of the equation $ax - by = c$ given by Āryabhata (born 476 A.D.) as well as by Brahmagupta and Bhāskara, though it anticipated Bachet's solution which is really equivalent to our method of solution by continued fractions, is an easy development from Euclid's method of finding the greatest common measure or proving by that process that two numbers have no common factor (Eucl. VII. 1, 2, X. 2, 3)[3], and it would be strange if the Greeks had not taken this step. The Indian solution of the equation $xy = ax + by + c$, by the geometrical form in which it was clothed, suggests Greek origin[4].

The "cyclic method" of solving the equation

$$x^2 - Ay^2 = 1$$

is found in Brahmagupta and Bhāskara[5] (born 1114 A.D.) and is well described by Hankel, Cantor and Konen[6].

The method is given in the form of dogmatic rules, without any proof of the assumptions made, but is equivalent to a preliminary lemma followed by the solution proper.

[1] Hankel, *Zur Geschichte der Math. im Alterthum und Mittelalter*, pp. 203–4.

[2] Tannery, "Sur la mesure du cercle d'Archimède" in *Mém. de la soc. des sciences phys. et nat. de Bordeaux*, II^e Sér. IV., 1882, p. 325; cf. Konen, pp. 27–28; Zeuthen, "L'Oeuvre de Paul Tannery comme historien des mathématiques" in *Bibliotheca Mathematica*, VI$_3$, 1905–6, pp. 271–273.

[3] G. R. Kaye, "Notes on Indian mathematics, No. 2, Āryabhata" in *Journal of the Asiatic Society of Bengal*, Vol. IV. No. 3, 1908, pp. 135–138.

[4] Cf. the description of the solution in Hankel, p. 199; Cantor, *Gesch. d. Math.* I$_3$, p. 631.

[5] The mathematical chapters in the works of these writers containing the solution in question are contained in H. T. Colebrooke's *Algebra with arithmetic and mensuration from the Sanskrit of Brahmegupta and Bhaskara*, London, 1817.

[6] Hankel, pp. 200–203; Cantor, I$_3$, pp. 632–633; Konen, *op. cit.*, pp. 19–26.

Lemma.

If $x=p$, $y=q$ be a solution of the equation

$$Ay^2+s=x^2,$$

and $x=p'$, $y=q'$ a solution of the equation

$$Ay^2+s'=x^2,$$

then, say the Indians, $x=pp'\pm Aqq'$, $y=pq'\pm p'q$ is a solution of the equation

$$Ay^2+ss'=x^2.$$

In other words, if

$$\left.\begin{aligned} Aq^2+s&=p^2\\ Aq'^2+s'&=p'^2\end{aligned}\right\},$$

then $$A(pq'\pm p'q)^2+ss'=(pp'\pm Aqq')^2.$$

This is easily verified[1].

In particular, taking $s=s'$, we find, from any solution $x=p$, $y=q$ of the equation

$$Ay^2+s=x^2,$$

a solution $x=p^2+Aq^2$, $y=2pq$ of the equation

$$Ay^2+s^2=x^2.$$

Again, particular use of the lemma can be made when $s=\pm 1$ or $s=\pm 2$.

(*a*) If $s=+1$, and $x=p$, $y=q$ is a solution of

$$Ay^2+1=x^2,$$

then $x=p^2+Aq^2$, $y=2pq$ is another solution of the same equation.

If $s=-1$, and $x=p$, $y=q$ is a solution of

$$Ay^2-1=x^2,$$

then $x=p^2+Aq^2$, $y=2pq$ is a solution of

$$Ay^2+1=x^2.$$

(*b*) If $s=\pm 2$, and $x=p$, $y=q$ is a solution of

$$Ay^2\pm 2=x^2,$$

then $x=p^2+Aq^2$, $y=2pq$ is a solution of

$$Ay^2+4=x^2.$$

In this case, since $2pq$ is even, the whole result when the values of x, y are substituted must be divisible by 4, and we have $x=\frac{1}{2}(p^2+Aq^2)$, $y=pq$ as a solution of the equation

$$Ay^2+1=x^2.$$

[1] For, since $s=p^2-Aq^2$, $s'=p'^2-Aq'^2$,

$$\begin{aligned} ss'&=(p^2-Aq^2)(p'^2-Aq'^2)\\ &=(pp')^2+(Aqq')^2-A(pq')^2-A(p'q)^2\\ &=\{(pp')^2\pm 2App'qq'+(Aqq')^2\}-A\{(pq')^2\pm 2pp'qq'+(p'q)^2\}\\ &=(pp'\pm Aqq')^2-A(pq'\pm p'q)^2.\end{aligned}$$

Solution proper of the equation $x^2 - Ay^2 = 1$.

We take two numbers prime to one another, p, q, and a third number s with no square factor, such that

$$Aq^2 + s = p^2,$$

the numbers being also chosen (in order to abbreviate the solution) such that s is as small as possible, though this is not absolutely necessary. (This is a purely empirical matter; we have only to take a rough approximation to $\sqrt{A}$ in the form of a fraction p/q.)

[It follows that s, q can have no common factor; for, if δ were a common factor of s, q, it would also be a factor of p^2, and p^2, q^2 would have a common factor. But p, q are prime to one another.]

Now find a number r such that

$$q_1 \equiv \pm\frac{p+qr}{s} \text{ is a whole number.}$$

[This would be done by the Indian method called *cuṭṭaca* ("pulveriser"), corresponding to our method by continued fractions.]

Of the possible values of r a value is taken which will make $r^2 - A$ as small as possible.

Now, say the Indians, we shall have:

$$s_1 = \pm\frac{r^2 - A}{s} \text{ is an integral number,}$$

and

$$Aq_1^2 + s_1 = \left(\frac{pq_1 - 1}{q}\right)^2 = p_1^2.$$

(Again the proofs are not given; they are however supplied by Hankel[1].)

[1] Since $q_1 = \frac{p+qr}{s}$ is an integral number, all the letters in $q_1 s = p + qr$ represent integers.

Further, $$s = p^2 - Aq^2;$$
therefore, eliminating s, we have
$$q_1(p^2 - Aq^2) = p + qr,$$
or
$$p(pq_1 - 1) = q(r + Aqq_1).$$

Since p, q have no common factor, q must divide $pq_1 - 1$; that is,

$$\frac{pq_1 - 1}{q} = \text{an integer.}$$

We have next to prove that $s_1 = (r^2 - A)/s$ is an integer.

Now $$r^2 - A = \frac{(q_1 s - p)^2 - Aq^2}{q^2} = \frac{q_1^2 s^2 - 2pq_1 s + s}{q^2}, \text{ since } s = p^2 - Aq^2;$$

therefore $$\frac{s(q_1^2 s - 2pq_1 + 1)}{q^2} \text{ is an integer,}$$

and, since s, q have no comn on factor, it follows that

$$\frac{q_1^2 s - 2pq_1 + 1}{q^2} = \frac{r^2 - A}{s} \text{ is an integer.}$$

Also $$s_1 = \frac{r^2 - A}{s} = \frac{q_1^2 s - 2pq_1 + 1}{q^2} = \frac{q_1^2(p^2 - Aq^2) - 2pq_1 + 1}{q^2} = \left(\frac{pq_1 - 1}{q}\right)^2 - Aq_1^2.$$

We have therefore satisfied a new equation of the same form as that originally taken[1].

We proceed in this way, obtaining fresh results of this kind, until we arrive at one in which $s = \pm 1$ or ± 2 or ± 4, when, by means of the lemma, we obtain a solution of

$$Ay^2 + 1 = x^2.$$

Example. To solve the equation $67y^2 + 1 = x^2$.

Since 8^2 is the nearest square to 67, we take as our first auxiliary equation $67 . 1^2 - 3 = 8^2$, so that $p = 8$, $q = 1$, $s = -3$.

Thus $q_1 = -\dfrac{8+r}{3}$. We put $r = 7$, which makes q_1 an integer and at the same time makes $s_1 = -\dfrac{7^2 - 67}{3} = 6$ as small as possible.

Thus $$q_1 = -5, \; p_1 = (pq_1 - 1)/q = -41,$$
and we have satisfied the new equation

$$67 . 5^2 + 6 = 41^2.$$

Next we take $q_2 = \dfrac{41 + 5r_2}{6}$, and we put $r_2 = 5$, giving $q_2 = 11$; thus $s_2 = \dfrac{r_2^2 - 67}{6} = -7$, and $p_2 = (p_1q_2 - 1)/q_1 = 90$, and

$$67 . (11)^2 - 7 = 90^2.$$

Next $q_3 = -\dfrac{90 + 11r_3}{7}$, and we put $r_3 = 9$, giving $q_3 = -27$; therefore

$$s_3 = \frac{r_3^2 - 67}{-7} = -2, \quad p_3 = \frac{-90 . 27 - 1}{11} = -221, \text{ and}$$

$$67 . (27)^2 - 2 = (221)^2.$$

As we have now brought our s down to 2, we can use the lemma, and

$$67 (2 . 27 . 221)^2 + 4 = (221^2 + 67 . 27^2)^2,$$

or $$67 (11934)^2 + 4 = (97684)^2;$$
therefore, dividing by 4, we have

$$67 (5967)^2 + 1 = (48842)^2.$$

Of this Indian method Hankel says, "It is above all praise; it is certainly the finest thing which was achieved in the theory of numbers

[1] Hankel conjectures that the Indian method may have been evolved somewhat in this way.

If $Aq^2 + s = p^2$ is given, and if we put $Aq'^2 + s' = p'^2$, then

$$A(pq' - p'q)^2 + ss' = (pp' - Aqq')^2.$$

Now suppose p', q' to be determined as whole numbers from the equation $pq' - p'q = 1$, and let the resulting integral value of $pp' - Aqq'$ be r.

Then $A + ss' = r^2$, and accordingly $r^2 - A$ must be divisible by s, or $s' = (A - r^2)/s$ is a whole number.

Eliminating p' from the two equations in p', q', we obtain

$$q' = (p + qr)/(p^2 - Aq^2) = (p + qr)/s,$$

and, as stated in the rule. r has therefore to be so chosen that $(p + qr)/s$ is an integer.

before Lagrange"; and, although this may seem an exaggeration when we think of the extraordinary achievements of a Fermat, it is true that the Indian method is, remarkably enough, the same as that which was rediscovered and expounded by Lagrange in his memoir of 1768[1]. Nothing is wanting to the cyclic method except the proof that it will in every case lead to the desired result whenever A is a number which is not a square; and it was this proof which Lagrange first supplied.

Fermat.

As we have already said, Fermat rediscovered our problem and was the first to assert that the equation

$$x^2 - Ay^2 = 1,$$

where A is any integer not a square, always has an unlimited number of solutions in integers.

His statement was made in a letter to Frénicle of February, 1657[2]. Fermat asks Frénicle for *a general rule for finding, when any number not a square is given, squares which, when they are respectively multiplied by the given number and unity is added to the product, give squares.* If, says Fermat, Frénicle cannot give a general rule, will he give the smallest value of y which will satisfy the equations $\boxed{61y^2 + 1 = x^2}$ and $\boxed{109y^2 + 1 = x^2 ?}$[3]

At the same time Fermat issued a challenge to the same effect to mathematicians in general, prefacing it by some remarks which are worth quoting in full[4].

"There is hardly any one who propounds purely arithmetical questions, hardly any one who understands them. Is this due to the fact that up to now arithmetic has been treated geometrically rather than arithmetically? This has indeed generally been the case both in ancient and modern works; even Diophantus is an instance. For, although he has freed himself from geometry a little more than others have in that he confines his analysis to the consideration of rational numbers, yet even there geometry is not entirely absent, as is sufficiently proved by the *Zetetica* of Vieta, where the method of Diophantus is extended to continuous magnitude and therefore to geometry.

"Now arithmetic has, so to speak, a special domain of its own, the theory of integral numbers. This was only lightly touched upon by Euclid in his *Elements*, and was not sufficiently studied by those who followed him (unless, perchance, it is contained in those Books of Diophantus of

[1] "Sur la solution des problèmes indéterminés du second degré" in *Mémoires de l'Acad. Royale des Sciences et Belles-Lettres de Berlin*, t. XXIII. 1769 (= *Oeuvres de Lagrange*, II. pp. 377 sqq.). The comparison between Lagrange's procedure and the Indian is given by Konen, pp. 75–77.

[2] *Oeuvres de Fermat*, II. pp. 333–4.

[3] Fermat evidently chose these cases for their difficulty; the smallest values satisfying the first equation are $y = 226153980$, $x = 1766319049$, and the smallest values satisfying the second are $y = 15140424455100$, $x = 158070671986249$.

[4] *Oeuvres de Fermat*, II. pp. 334–5.