THE DIOPHANTINE EQUATION $y^2-k=x^3$.

By L. J. MORDELL.

[Read December 14th, 1912.—Received January 13th, 1913.—Revised May 14th, 1913.]

1. This equation was brought into prominence by Fermat,* who had proposed as a problem to the English mathematicians, to shew that there was only one integral solution of the equation $y^2+2=x^3$. Concerning this he† says: "Peut on trouver en nombres entiers un carré autre que 25, qui, augmenté de 2, fasse un cube? A la première vue cela paraît d'une recherche difficile, en fractions une infinité de nombres se déduisent de la méthode de Bachet; mais la doctrine des nombres entiers, qui est assurément très-belle et très-subtile, n'a été cultivée ni par Bachet, ni par aucun autre dont les écrits venus jusqu'à moi." He did not publish his method, which is not known at present.

We shall consider the equation from three points of view. Firstly, we shall find general formulæ for k, for which there are no solutions (we consider integral values only of the unknowns throughout our paper); secondly, we shall apply ideal numbers; and, finally, we shall make use of the arithmetical theory of the binary cubic.

In a series of notes and papers published by Lebesgue,‡ Gerono,§ Jonquières,‖ Realis,¶ and Pepin,** †† various values and formulæ have been given for k for which our equation is insoluble. These results can be considerably extended. Moreover, the same method supplies us with a very useful tentative method for solving such equations.‡‡

---

* Ball, *Mathematical Recreations*, p. 40.

† Brassinne's *Précis*, p. 122, or Fermat's *Diophantus*, Bk. VI, Prop. 19, p. 320.

‡ *Nouvelles Annales de Mathématiques*, 1st series, Vol. 9, 1850; 2nd series, Vol. 8, 1869.

§ *Ibid.*, 2nd series, Vol. 8, 1869; Vol. 9, 1870; Vol. 10, 1871; Vol. 16, 1877.

‖ *Ibid.*, Vol. 17, 1878.

¶ *Ibid.*, Vol. 22, 1883.

** Liouville, *Journal de Math. pures et appliquées*, 3rd series, Vol. 1, 1875.

†† *Annales de la Société Scientifique de Bruxelles*, 1882, Pt. 2.

‡‡ Cf. Cunningham, *Educational Times Reprints*, Vol. 13, Question 15697, and Vol. 14, Question 16408.

2. A few preliminary considerations are necessary. It is well known that if p is any odd prime factor of x^2-ky^2, then $x^2 \equiv ky^2 \bmod p$; so that, if p is prime to ky, $(k/p)=1$. Thus, by the use of the law of quadratic reciprocity and the supplementary laws, we find that p is congruent to certain residues to mod k or mod $4k$. And any prime q such that $(k/q)=-1$ cannot be a divisor of x^2-ky^2 unless it divides both x and y. Hence any odd number t such that $(k/t)=-1$ cannot be a divisor of x^2-ky^2 unless all the prime factors q of t, for which $(k/q)=-1$, divide both x and y.

Consider now the equation

$$\begin{aligned} y^2-klb^2 &= x^3-k^3a^3 \\ &= (x-ka)\,N, \end{aligned} \tag{1}$$

where k has no square factors and is prime to bl. Moreover, $N=x^2+kax+k^2a^2$ is essentially positive, and a will be hereafter so chosen that N is odd.

Then $$y^2 \equiv klb^2 \bmod N,$$

and so $(kl/N)=1$ if N is prime to klb^2. Now N is prime to k if x is so, and from (1) we see that this is the case, since k is prime to bl. As to N being prime to $l(\neq \pm 1)$, this is best postponed to the stage when particular values of l are considered; but this will always be the case.

If now N is prime to b, then, since $(N/k)=1$, we find

$$\begin{aligned} (l/N) &= (k/N)(N/k) \\ &= (-1)^{\frac{1}{2}(k-1)(N-1)}, \end{aligned} \tag{2}$$

if k is positive, and it is also true if k is negative. If, therefore, values of a and b can be chosen such that for given k and l, (2) is untrue, it will follow that (1) is insoluble. In particular, when $l=1$, (1) is insoluble, if $N \equiv 3 \bmod 4$ and $k \equiv 3 \bmod 4$. If, further, $k=-1$, (2) is replaced by $(-1/N)=1$, and here again (1) is insoluble if $N \equiv 3 \bmod 4$.

Now suppose (2) is untrue, *i.e.* $(kl/N)=-1$, then from (1), since $y^2-klb^2 \equiv 0 \bmod N$, it follows that b and N have a common prime factor q such that $(kl/q)=-1$. Putting $y=qy_1$, $b=qb_1$, we have

$$y_1^2-klb_1^2=(x-ka)\,N/q^2. \tag{3}$$

But, since $N=x^2+kax+k^2a^2 \equiv 0 \bmod q$,

$$(x-ka)^2+3kax \equiv 0 \bmod q.$$

Hence $x-ka$ is prime to q if $3kax$ is so. Now a is prime to q if a and b have no common factors of the type q; 3 is prime to q if $b \not\equiv 0 \bmod 3$ when $(kl/3) = -1$; k is prime to q, since b and k are prime to each other. Moreover, x is prime to q, since ka is so. Hence $x-ka$ is prime to q, and hence $N \equiv 0 \bmod q^2$. But, putting $N = M_1 q^2$, we see that $(kl/M_1) = -1$.

Continuing this process, we can remove all the factors of b typified by q, and finally arrive at an equation of the form

$$Y^2 - klB^2 = (x-ka)M,$$

where $(kl/M) = -1$; but B and M have no common factors q such that $(kl/q) = -1$. Hence the equation is impossible. But $(kl/N) = (kl/M)$. Hence, if (2) is untrue the equation (1) is insoluble if a and b have no common prime factors q such that $(kl/q) = -1$, and $b \not\equiv 0 \bmod 3$ if $(kl/3) = -1$. We may note that the equation (1) is still insoluble even if a and b possess common factors of the type q, provided the indices of these factors satisfy certain conditions which are easily found in any particular case.

Let us now consider (1) when $l = 1$, so that our equation becomes

$$y^2 - kb^2 = x^3 - k^3a^3. \tag{3a}$$

We suppose $k \equiv 3 \bmod 4$, free from square factors and prime to b. Also a and b have no common prime factors q for which $(k/q) = -1$, and $b \not\equiv 0 \bmod 3$ if $(k/3) = -1$. Hence (3a) is insoluble if a and b are such that $N \equiv 3 \bmod 4$.

We now solve the congruence

$$x^2 + kax + k^2a^2 \equiv 3 \bmod 4 \text{ (or since } k \equiv 3 \bmod 4),$$

$$x^2 - ax + a^2 \equiv 3 \bmod 4.$$

Hence, if $a \equiv 1$, then $x \equiv -1, 2$
„ $a \equiv 2$, „ $x \equiv -1, 1$
„ $a \equiv 3$, „ $x \equiv 1, 2$ } . (4)

If we now take any one of these values of a mod 4 and can find values of b such that x satisfying (3) must be congruent to one or both of the corresponding residues mod 4 given in (4), then (3) is insoluble for these values of a and b.

But $$y^2 \equiv x^3 + a^3 - b^2 \bmod 4,$$

and if we take $a \equiv -1 \bmod 4$ and $b \equiv 0 \bmod 2$, then $x \equiv 1 \bmod 4$. Hence we have the first insoluble equation

$$y^2 = x^3-k^3(4a-1)^3+4kb^2.$$

Take $a \equiv 2 \bmod 4$ and $b \equiv 1 \bmod 2$, then $x \equiv 1 \bmod 4$, and hence the insoluble equation

$$y^2 = x^3-k^3(4a+2)^3+k(2b+1)^2.$$

Take $a \equiv 2 \bmod 4$ and $b \equiv 0 \bmod 2$, then $x \equiv 1 \bmod 4$ or even; so if we can find values of a and b satisfying these congruences, and also such that x cannot be even,* then (3) is insoluble.

Now when $A \equiv 4 \bmod 8$, and

$$y^2 = x^3+A$$

admits of even values for x, we have $y \equiv 2 \bmod 4$, whence

$$A \equiv 12 \bmod 16 \text{ or } \equiv 4 \bmod 32,$$

i.e.

$$A \not\equiv -12 \bmod 32.$$

Hence the values of a and b needed are given by

$$-k^3a^3+kb^2 \equiv -12 \bmod 32,$$

from which we obtain

$$a \equiv -k-3 \bmod 8 \text{ and } b \equiv 2 \bmod 4,$$

and hence the insoluble equation

$$y^2 = x^3-k^3(5+8c-k)^3+4k(2b+1)^2.$$

Finally, taking $a \equiv 1 \bmod 4$ and $b \equiv 0 \bmod 2$, then $x \equiv 3 \bmod 4$ or even. The equation (3) becomes, writing $4a+1$ for a and $2b$ for b,

$$y^2 = x^3-k^3(4a+1)^3+4kb^2 = x^3+A,$$

say, and x cannot be even if $A \equiv 5 \bmod 8$. This gives us

$$4a+1 \equiv 4b^2+3k \bmod 8,$$

and we have the insoluble equation

$$y^2 = x^3-k^3(4b^2+3k+8c)^3+4kb^2,$$

---

* We shall have frequent occasion to use equations of the form $y^2 = x^3+k$, which do not admit of even values for x. This is the case when $k \equiv 5 \bmod 8$, $k \equiv -12 \bmod 32$ and also $k \equiv -16$ or $32 \bmod 64$.

which is equivalent to the two equations

$$y^2 = x^3 - k^3(3k+8c)^3 + 16kb^2,$$

$$y^2 = x^3 - k^3(4+3k+8c)^3 + 4k(2b+1)^2.$$

In particular, by taking $k = -1$, we find some of the known insoluble equations $y^2 = x^3 + A^3 - B^2$, say, and our conditions become $B \not\equiv 0 \bmod 3$, and A and B have no common prime factor congruent to 3 mod 4. We thus find the insoluble equations $y^2 + k = x^3$ where $k = 9, 3, 12, 43, 91, 99$, and $-k = 95, 47, 39, 11, 67, 53, 13, 20$.

3. Taking now $l = 2$ in equation (1), and following the same procedure as before, we find the insoluble equations

$$y^2 = x^3 - k^3a^3 + 2kb^2,$$

when (1) $a \equiv 2, 4 \bmod 8$, $b \equiv 1 \bmod 2$,

(2) $a \equiv 4 \bmod 8$, $b \equiv 4 \bmod 8$,

(3) $a \equiv 2 + 4(-1)^{\frac{1}{2}(k-1)} \bmod 16$, $b \equiv 2 \bmod 4$,

and k is odd, free from square factors and prime to b. Also $b \not\equiv 0 \bmod 3$, when $(k/3) = 1$, and a and b have no common prime factor q for which $(2k/q) = -1$. As particular cases, when $k = \pm 1$, we find the insoluble equations $y^2 + k = x^3$, where $k = 62, 98$, and $-k = 62, 46, 32, 66, 90, 96$.

When $l = 3$, we find the insoluble equations

$$y^2 = x^3 - k^3a^3 + 3kb^2,$$

when (1) $a \equiv 1 \bmod 4$, $b \equiv 0 \bmod 2$,

(2) $a \equiv 2 \bmod 4$, $b \equiv 1 \bmod 2$,

(3) $a \equiv 2(-1)^{\frac{1}{2}(k+3)} \bmod 8$, $b \equiv 2 \bmod 4$,

(4) $a \equiv 5k - 2(-1)^{\frac{1}{2}b} \bmod 8$, $b \equiv 0 \bmod 2$,

where $k \equiv 1 \bmod 4$, free from square factors and prime to $3b$. Also a and b have no common odd prime factor to q such that $(3k/q) = -1$, and b is prime to 3. When $k = 1$, we find the insoluble equations $y^2 - k = x^3$, $k = 75, 84$.

Finally, when $l = 6$, we find the insoluble equations

$$y^2 = x^3 - k^3a^3 + 6kb^2,$$

when (1) $a \equiv -2, 4 \bmod 8$, $b \equiv 1 \bmod 2$,

(2) $a \equiv 4 \bmod 8$, $b \equiv 4 \bmod 8$,

(3) $a \equiv 6+4(-1)^{\frac{1}{2}(k-1)} \bmod 16$, $b \equiv 2 \bmod 4$,

where k is an odd number possessing no square factors, and k and b are prime to each other and to 3. Also a and b have no common prime factor q, such that $(6k/q) = -1$.

4. These results can be immediately extended to equations of higher degrees. Thus we have the insoluble equation

$$y^2 = x^{2n+1}-k^{2n+1}a^{2n+1}+kb^2,$$

where $a \equiv 2 \bmod 4$ and $b \equiv 1 \bmod 2$, and k satisfies the conditions of equation (3a). Further $2n+1$, a possible common factor of $x-ka$, and $(x^{2n+1}-k^{2n+1}a^{2n+1})/(x-ka)$, plays the same part in the remaining conditions that 3 does.

Another insoluble equation is

$$y^2 = x^{4n+3}-k^{4n+3}a^{4n+3}+kb^2,$$

where $a \equiv -1 \bmod 4$, $b \equiv 0 \bmod 2$, and with similar conditions to those above. The proof of these equations is very simple. We give no more of them as it is simply rewriting our previous results with slight changes. We may, however, notice the insoluble equations

$$y^2 = x^{4n+3}+k,$$

when (1), $k = -1-4b^2$ and b and $4n+3$ have no common prime factors congruent to 3 mod 4; (2) $k = -1+12b^2$, b is prime to 3 and b and $4n+3$ have no common prime factors congruent to $\pm 5 \bmod 12$; and finally when $k = 1+12(2b+1)^2$ and $2b+1$ is prime to 3, and $2b+1$ and $4n+3$ have no common prime factors congruent to $\pm 5 \bmod 12$.

5. The preceding impossible equations which we have given are very simple. We can obtain more complicated ones as follows. Suppose

$$y^2 = x^3+8k+5.$$

Here $x \equiv -1 \bmod 4$, *i.e.*, $x \equiv -1, 3 \bmod 8$.

If this equation can be written in the two ways

$y^2-2b^2 = (x+a)(x^2-ax+a^2)$, where $a \equiv 3 \bmod 8$, $b \equiv 1 \bmod 2$,

and

$y^2-8d^2 = (x+c)(x^2-cx+c^2)$, ,, $c \equiv -3 \bmod 8$, $d \equiv 1 \bmod 2$,

where our usual conditions are satisfied by a, b and c, d, we see that $x \equiv -1 \bmod 8$ is excluded by the first form of the equation, while $x \equiv 3 \bmod 8$ is excluded by the second form. Hence the equation is insoluble.

To find values for k, we have

$$b^2-4d^2 = \tfrac{1}{2}(c^3-a^3).$$

We can easily find an indefinite number of solutions of this equation. We easily find $a \equiv c \bmod 2$, and take any values for a and c consistent with this condition. We then split $\frac{1}{2}(c^3-a^3)$ into two factors p and q say, and take

$$b+2d = p,$$

$$b-2d = q.$$

In particular we may take

$$2p = c-a \quad \text{and} \quad q = c^2+ac+a^2,$$

or, again,

$$2p = c^3-a^3 \quad \text{and} \quad q = 1.$$

Thus we find insoluble equations, provided that the value we find for b, viz., $\frac{1}{2}(p+q)$ and the assumed value of a; and likewise d and c satisfy our usual conditions.

As a particular case of this equation consider

$$y^2 = x^3+45.$$

We note that x is prime to 3, and throwing the equation in the two forms

$$y^2-18 = (x+3)(x^2-3x+9),$$

$$y^2-72 = (x-3)(x^2+3x+9),$$

we see that when $x \equiv -1 \bmod 8$, $x^2-3x+9 \equiv 5 \bmod 8$, and prime to 3. This excludes $x \equiv -1 \bmod 8$. Similarly, when $x \equiv 3 \bmod 8$, from the second form of the equation. Hence it is insoluble.

By similar methods we can shew $y^2 = x^3+k$ is insoluble for

$$k = -24,\ 29,\ -36,\ 51,\ 59,\ 85,\ \pm 88,\ -92,\ 93.$$

Many of these can also be proved by the methods introduced in the latter part of the paper.

6. We can now give a tentative method for finding solutions of

$$y^2 = x^3+k.$$

We find $x \equiv p, q, r, \ldots \bmod 8$. If the equation can be written in any of the forms

$$y^2 = x^3+a^3-b^2 \quad \text{or} \quad y^2 = x^3+a^3 \pm 2b^2,$$

we may be able to exclude $x \equiv p, q, \ldots \bmod 8$, and are left with $x \equiv s, \ldots \bmod 8$.

We now carry out the same process with other moduli, say 3, 5, 7, &c., giving us $x \equiv t, \ldots \bmod 3$, &c. We then gather our results together and find $x \equiv A, B, \ldots \bmod N$, where the density of the values of x is considerably diminished. We now test the values of x as follows. We take another modulus M say, find the residues of $x \bmod M$ and reject those for which x^3+k is a non-quadratic residue of M. We may also find additional information, if the equation can be written in the form

$$y^2 \pm 2, 3, 5, \ldots Mb^2 = x^3+a^3.$$

Finally, if the necessary conditions are satisfied for many moduli M, we test the value of x by actual substitution. When $k=-31$, we find that there are no solutions with $x < 10^9$.

7. We shall now pass on to other methods, and give the first direct method for determining in many cases, sufficient conditions for the insolubility of our equation. We shall also shew the existence of new classes of equations of our type admitting a limited number only of solutions.

It would be interesting to know, if the method given below was that used by Fermat for his equation $y^2+2=x^3$. He knew, it is thought, that all factors of numbers of the form a^2+2b^2 are of the same form, but further proof is required before one can say that the complete solution of his equation is given by

$$x = a^2+2b^2, \quad y+\sqrt{(-2)} = [a+b\sqrt{(-2)}]^3.$$

As a matter of fact, Euler* himself has fallen into error on this point, with a similar equation. It is very curious that the application of ideal numbers has been overlooked, especially as Pepin's† paper is chiefly concerned with the equation

$$y^2+kz^2 = x^m,$$

and Dirichlet‡ had considered similar equations.

---

* *Algebra*, Pt. 2, Chap. 12.

† Liouville, 1875.

‡ *Collected Works*, "De Quelques Equations du cinquième degré," Vol. 1, p. 31.

8. We suppose k negative, free from square factors, and congruent to 2, 3, mod 4, so that x is prime to $2k$. Further let h, the number of classes of ideal numbers of determinant k, which is here the number of properly primitive classes of determinant k, be not divisible by 3. Then the equation has no solutions, unless $-k = 3a^2 \pm 1$, when it has but one.

Since $y^2-k = x^3$, writing $\theta = \sqrt{k}$, we have

$$(y+\theta)(y-\theta) = x^3.$$

But any common factor of $y+\theta$ and $y-\theta$ is a factor of 2θ, and since x is prime to 2θ, it follows that any prime ideal factor of x cannot be a factor both of $y+\theta$ and $y-\theta$; consequently its cube must be a factor either of $y+\theta$ or of $y-\theta$. And since the only units in the domain of θ are ± 1, and $\pm i$ when $k = -1$, and as -1 and $\pm i$ can be absorbed in T_1^3, we obtain

$$y+\theta = T_1^3,$$

$$y-\theta = T_2^3,$$

where T_1 and T_2 are ideal numbers in the domain of θ. But since $h \not\equiv 0 \bmod 3$, T_1 and T_2 are primary numbers, and we can write

$$T_1 = a+b\theta, \quad T_2 = a-b\theta,$$

and so $$y+\theta = (a+b\theta)^3, \quad \text{and} \quad x = a^2-kb^2.$$

Therefore $$1 = b(3a^2+kb^2),$$

whence $$b = \mp 1,$$

and $$-k = 3a^2 \pm 1,$$

also $$x = 4a^2 \pm 1.$$

As illustrations,

for $k = -2$, the only solution is $x = 3$, $y = 5$,

„ $k = -13$, „ „ $x = 17$, $y = 70$,

„ $k = -74$, „ „ $x = 99$, $y = 985$,

while there are none for $-k = 5, 6, 10, 14, 17, 21, 22, 30, 33, 34, 37, 41, 42, 46, 57, 58, 65, 66, 69, 70, 73, 77, 78, 82, 85, 86, 90, 93, 94, 97$.

Similar results hold when $k \equiv 5 \bmod 8$, $k \neq -3$, for which h is equal to the number of improperly primitive classes of determinant k (or $\frac{1}{3}$ the number of properly primitive classes of determinant k). Also when $k \equiv 1 \bmod 8$, for which h is equal to the number of properly primitive

classes of determinant k. But now there is great difficulty in dealing with the case of x being even, though our method applies to the odd values of x.

We have $$y+\theta=(a+b\phi)^3,$$

where $$2\phi=-1+\sqrt{k},$$

and $$x=a^2-ab+\tfrac{1}{4}(1-k)\,b^2.$$

Therefore $$8=b\,[3(2a-b)^2+kb^2].$$

Hence either $b=\mp 1$ and $-k=3(2a\pm 1)^2\pm 8$,

or $b=\mp 2$ and $-k=3(a\pm 1)^2\pm 1$.

Thus the equation is insoluble for

$$-k=43,\ 51,\ 91.$$

Also $-k=11$ gives only $x=3,\ y=4,$ and $x=15,\ y=58,$

$-k=19$,, $x=7,\ y=18,$

$-k=35$,, $x=11,\ y=36,$

$-k=67$,, $x=23,\ y=110.$

These results can be extended to equations of the form

$$y^2-kf^2=x^3,$$

where f is such that x is prime to $2kf$, and k satisfies the previous conditions. Thus when $k\equiv 2,\ 3 \mod 4$, we must have

$$f=b(3a^2+kb^2),$$

$$x=a^2-kb^2,$$

and when $k\equiv 1,\ 5 \mod 8,\quad k\neq -3,$

$$8f=b\,[3\,(2a-b)^2+kb^2],$$

$$x=a^2-ab+\tfrac{1}{4}(1-k)\,b^2,$$

and the equation either has no solutions or only a limited number.

In particular, when $f=4$, and $k\equiv 2,\ 3 \mod 4$, x is prime to $2k$, whence $4=b(3a^2+kb^2)$, which is easily seen to require $b=\mp 1$ and $-k=3a^2\pm 4$. Thus we have no solutions of $y^2+16k=x^3$ for $k=1,\ 2,\ 5,\ 6$.

Or, again, when $k\equiv 5 \mod 8$, and $f=2$, x is prime to $2k$, hence

$$16=b\,[3\,(2a-b)^2+kb^2],$$

hence, if $b = \mp 1$, $\quad -k = 3(2a \pm 1)^2 \pm 16$,

$b = \mp 2$, $\quad -k = 3(a \pm 1)^2 \pm 2$,

$b = -4$, $\quad -4k = 3(a+2)^2+1$.

Thus, for $y^2+4k = x^3$,

$k = 11$ gives only $x = 5,\ y = 9$,

$k = 19$ „ $x = 5,\ y = 7$, and $x = 101,\ y = 1015$.

Other illustrations are given by

$$y^2+52 = x^3 \quad \text{and} \quad y^2+68 = x^3.$$

For, if x is even, $x \equiv 2 \bmod 4$, and this value is excluded by putting the equations under the forms

$$y^2+25 = (x-3)(x^2+3x+9) \quad \text{and} \quad y^2+4 = (x-4)(x^2+4x+16),$$

and noting that $x-3 \equiv 3 \bmod 4$,

and that $x^2+4x+16 \equiv 12 \bmod 16$.

Further, h for 13 or 17, $\not\equiv 0 \bmod 3$, and $2 = b(a^2+kb^2)$ for $-k = 13, 17$ has no solutions, and hence the equations have none.

9. The simplicity of these results is due to the fact that the only units are ± 1, except for the determinants -1, where no inconvenience is caused, and -3 which was excluded from the discussion. We have, however, interesting results when the units must be taken into account.

Thus, let $y^2-kf^2 = x^3$, where $k \equiv 2, 3 \bmod 4$, free from square factors and positive, $h \not\equiv 0 \bmod 3$, and f is such that x is prime to $2kf$ (*e.g.*, if $f = 1$). Also let the unit for which U^* has its least non-zero value be given by $T^2-kU^2 = 1$. We easily find

$$x = a^2-kb^2 \quad \text{and} \quad y+f\sqrt{k} = (a+b\sqrt{k})^3,$$

which will give none, or a finite number of values for x; or

$$y+f\sqrt{k} = (T+U\sqrt{k})(a+b\sqrt{k})^3.$$

This is fairly obvious if $T+U\sqrt{k}$ is the fundamental unit ϵ. If it is not,

---

* We refer to this as the first solution, and similarly for the equation $T^3-kU^3 = 4$. Solutions for the first equation may be found in the tables at end of Vol. 1 of Legendre's *Théorie des Nombres*. For $T^2-kU^2 = 4$, see Cayley, *Crelle*, Vol. 53, p. 371.

putting $\epsilon\epsilon_1=-1$, we have

$$y+f\sqrt{k}=\epsilon(a+b\sqrt{k})^3.$$

Also $\epsilon=\epsilon^3\epsilon_1^2$, and ϵ^3 can be absorbed in $(a+b\sqrt{k})^3$.

We now consider different cases arising from the residues of kf^2 mod 9. Thus, let $kf^2\equiv 4, 7 \bmod 9$. This gives $x\equiv 0 \bmod 3$, and $k\equiv 1 \bmod 3$.

Hence $$x\equiv a^2-b^2\equiv 0 \bmod 3,$$

$$f=U(a^3+3kab^2)+T(3a^2b+kb^3).$$

But since $$T^2-kU^2=1,$$

and $k\equiv 1 \bmod 3$; $U\equiv 0 \bmod 3$ and $T^2\equiv 1 \bmod 9$.

Hence $$f\equiv Tkb^3 \bmod 3$$

$$\equiv Tkb \quad ,,$$

Thus $$b\equiv Tf \quad ,,$$

and $$a^2\equiv 1 \quad ,,$$

Hence $$f\equiv Ua^3+3T^2a^2f+T^4f^3k \bmod 9,$$

or $$f\equiv Ua^3+3f+f^3k \quad ,,$$

or $$0\equiv Ua^3+f(2+kf^2) \quad ,,$$

Hence our equation is insoluble if

$$kf^2\equiv 4 \bmod 9, \quad \text{and} \quad U\equiv 0 \bmod 9,$$

$$kf^2\equiv 7 \bmod 9, \quad \text{and} \quad U\equiv \pm 3 \bmod 9.$$

And in particular the equations

$$y^2-k=x^3, \quad k=7, 34, 58, 70.$$

If, however, $k\equiv 1, 5 \bmod 8$, we find

$$y+f\sqrt{k}=\left[T_1+\frac{U_1}{2}(1+\sqrt{k})\right]\left[a_1+\frac{b_1}{2}(1+\sqrt{k})\right]^3,$$

$$x=a_1^2+a_1b_1+\tfrac{1}{4}(1-k)b_1^2,$$

$$1=T_1^2+T_1U_1+\tfrac{1}{4}(1-k)U_1^2,$$

and also the same equation with $T_1=1$, $U_1=0$. We dispose of this by saying, it can give only a finite number of values for x.

Putting
$$a = 2a_1 + b_1,$$
$$b = \quad b_1,$$
$$-T = 2T_1 + U_1,$$
$$-U = \quad U_1,$$

we find $2f \equiv U(a^3+3kab^2)+T(3a^2b+kb^3) \mod 9,$

$$x \equiv a^2-b^2 \equiv 0 \mod 3,$$
$$T^2-kU^2 = 4.$$

Hence $U \equiv 0 \mod 3, \quad T^2 \equiv 4 \mod 9, \quad b \equiv -Tf \mod 3,$

and $0 \equiv Ua^3-f(5+7kf^2) \mod 9.$

Hence our equation is insoluble if

$$kf^2 \equiv 4 \mod 9 \quad \text{and} \quad U \equiv 0 \mod 9,$$
$$kf^2 \equiv 7 \mod 9 \quad \text{and} \quad U \equiv \pm 3 \mod 9.$$

It will be noticed that these results are of the same form as the previous ones. We thus find the particular equations

$$y^2-k = x^3, \quad k = 61, 85.$$

For $kf^2 \equiv -4, -7 \mod 9, \quad k \equiv 2, 3 \mod 4,$

and $T^2-kU^2 = 1.$

Then $T^2+U^2 \equiv 1 \mod 3,$

and either T or $U \equiv 0 \mod 3.$

Carrying out the same process as before, we find if $T \equiv 0 \mod 3$, our equation is insoluble if

$$kf^2 \equiv -4 \mod 9 \quad \text{and} \quad T \equiv \pm 3 \mod 9,$$
$$kf^2 \equiv -7 \mod 9 \quad \text{and} \quad T \equiv 0 \mod 9.$$

We find exactly the same results when $U \equiv 0 \mod 3$, if we replace T by U in the above conditions. We also find the same results when

$$k \equiv 1 \mod 4,$$

but of course T and U are now given by

$$T^2-kU^2 = 4.$$

We now find the particular insoluble equations

$$y^2-k=x^3, \quad k=14, 23, 59, 83, 86.$$

For $kf^2 \equiv \pm 3 \bmod 9$, *i.e.*, $f^2 \equiv 1 \bmod 3$, and $k \equiv \pm 3 \bmod 9$, and for $k \equiv 2, 3 \bmod 4$, we have, as before,

$$T^2-kU^2=1,$$

$$f \equiv U(a^3+3kab^2)+T(3a^2b+kb^3) \bmod 9.$$

Thus our equation is impossible if $U \equiv 0 \bmod 3$. If this be not the case, and we take $k \equiv -3 \bmod 9$, we find

$$a \equiv fU \bmod 3.$$

Thus $$f \equiv f^3U^4+3bf^2U^2T-3Tb^3 \bmod 9,$$

or $$f(1-f^2U^4) \equiv 3bT(U^2-b^2) \bmod 9.$$

And since $b(U^2-b^2) \equiv 0 \bmod 3$ as $U \not\equiv 0 \bmod 3$, our equation is insoluble if $f^2U^4 \not\equiv 1 \bmod 9$, *i.e.*, $f \not\equiv \pm U \bmod 9$.

When $k \equiv 1 \bmod 4$, we find by putting $2f$ for f, the conditions $U \equiv 0 \bmod 3$ or $2f \not\equiv \pm U \bmod 9$, where $T^2-kU^2=4$.

In particular we have $y^2-k=x^3$ impossible for

$$k=6, 21, 42, 69, 78, 87, 93.$$

10. Another illustration is given by $y^2-60=x^3$. The even values of x satisfy $x \equiv 2 \bmod 4$, and this is excluded by putting the equation in the form

$$y^2+4=(x+4)(x^2-4x+16),$$

and noticing that the last factor is congruent to 12 mod 16. Hence x is prime to 30, and h for determinant 15 is 4. Also $f=2$, $U=\pm 1$, and $fU^2 \not\equiv \pm 1 \bmod 9$. Hence the impossibility of the equation.

And finally consider $y^2-27=x^3$. Firstly, let x be not divisible by 3. Then we have

$$y+3\sqrt{3}=(T+U\sqrt{3})(a+b\sqrt{3})^3 \quad \begin{cases} T=\pm 2, & U=\pm 1 \\ T=\pm 1, & U=0 \end{cases},$$

$$x=a^2-3b^2.$$

Thus $$3=U(a^3+9ab^2)+T(3a^2b+3b^3).$$

For $T=\pm 2$, this gives $a \equiv 0 \bmod 3$, contrary to our supposition For $U=0$, there are no solutions.

Secondly, put $x = 3\xi$, $y = 9\eta$, then

$$3\eta^2 - 1 = \xi^3.$$

Thus $$\sqrt{3}\,\eta + 1 = (T + U\sqrt{3})(a + b\sqrt{3})^3,$$

or $$1 = T(a^3 + 9ab^2) + 3U(3a^2b + 3b^3).$$

For $T = \pm 2$, this gives $1 \equiv \pm 2a^3 \mod 9$, which is absurd.
For $T = \pm 1$, this gives $x = -3$.

11. Other results may be found by considering congruences to mod 7. Thus for

$$y^2 - kf^2 = x^3, \quad k \equiv 2, 3 \mod 4,$$

where k and f satisfy our usual conditions and $kf^2 \equiv 4 \mod 7$, we easily find

$$x \equiv a^2 - kb^2 \equiv 0 \mod 7,$$

or $$a^2 f^2 \equiv 4b^2 \mod 7.$$

Thus $$a \equiv 2c \quad ,,$$

$$b \equiv \pm fc \quad ,,$$

Also $$f = U(a^3 + 3kab^2) + T(3a^2b + kb^3),$$

and we can shew that this equation is impossible if $U \equiv 0 \mod 7$. We have then

$$f \equiv T(3a^2b + kb^3) \mod 7,$$

or $$f \equiv \pm (12f + kf^3)c^3 \mod 7,$$

or $$1 \equiv \pm 2c^3 \mod 7,$$

which is absurd.

The same result holds when $k \equiv 1 \mod 4$, but of course U is now given by $T^2 - kU^2 = 4$.

12. We can also prove our results by the theory of the binary cubic,* which also has the advantage of throwing additional light upon our exceptional case, when the class number is divisible by 3.

Thus, let $y^2 - kf^2 = x^3$, where k possesses no square factors, and f is such that x is prime to $2kf$. Then when this equation has solutions, f can be properly represented by a binary cubic of determinant $4k$ (or what comes to the same thing, such cubics exist whose first coefficient is f);

* All that we need is contained in a paper by Arndt in *Crelle*, Vol. 53, p. 309.

and conversely, if such representations of f exist, our equation has solutions.

Taking the latter part first, consider the binary cubic (f, b, c, d) of determinant $4k$. Calling its Hessian (F, G, H), where

$$F=b^2-fc, \quad 2G=bc-fd, \quad H=C^2-bd, \quad k=G^2-FH,$$

we have by equating the coefficients of x^3 in the syzygy of the cubic,

$$(bF-fG)^2-kf^2=F^3,$$

which proves the second part.

Now suppose we have a solution of our original equation in the form $q^2-kf^2=F^3$. Hence we can find binary quadratics of determinant k, whose first coefficient is F. Let (F, G, H) be one of these, where we suppose G given by $fG \equiv -q \bmod F$. We shall now shew that we can find a binary cubic (f, b, c, d) of determinant $4k$, with (F, G, H) as its Hessian. It will be found that b, c, d are given by

$$\frac{1}{F}(q+Gf), \quad \frac{1}{F^2}(kf+2qG+fG^2), \quad \frac{1}{F^3}(kq+3kfG+3qG^2+fG^3).$$

It is easily seen that b is an integer. Also

$$\begin{aligned}(kf+2qG+fG^2)(kf-2qG+fG^2) &\equiv f^2(k+G^2)^2-4kf^2G^2 \bmod F^2,\\ &\equiv f^2(G^2-k)^2 \quad ,,\\ &\equiv 0 \quad ,,\end{aligned}$$

And these two factors have no factor in common with F since $4qG$ is prime to F; and remembering $fG \equiv -q \bmod F$, we find

$$kf+2qG+fG^2 \equiv 0 \bmod F,$$

and hence mod F^2, so that c is an integer. Similarly, we can shew that d is an integer, which proves the first part of our theorem.

13. When k is negative, and the class number (now and hereafter we mean by this the number of properly primitive classes of binary quadratics of determinant k) is not divisible by 3, the binary cubics are comprised in the class $(0, 1, 0, k)$, and hence we have either none or a limited number of proper representations of f, and hence none or a limited number of solutions of our original equation.

When k is positive, there are three classes of binary cubics corresponding to our given Hessian, and when the class number is not divisible by 3, only one of the classes consists of reducible cubics, while the other

two are improperly equivalent, and it suffices to consider only one of them.

Again, when k is negative and congruent to 2, 3 mod 4, and the index of irregularity for $k \not\equiv 0 \bmod 3$, then besides the principal form, there will be two other subtriplicate binary quadratic forms of determinant k. These two will be improperly equivalent, as also the binary cubics corresponding to them, and it suffices to consider only one of the latter. Now, if q, p is a solution of $q^2-k=p^3$, $(1, 0, -p, 2q)$ is a binary cubic of determinant $4k$, and if p is not represented by the principal quadratic form, which occurs when $-k = 3a^2 \pm 1$, $p = 4a^2 \pm 1$, $\pm q = 8a^3 \pm 3a$, this cubic and the one derived from it by changing the sign of q, constitute our classes of irreducible cubics of determinant $4k$. Hence under our conditions, when $-k \neq 3a^2+1$, all the solutions of $y^2-kf^2 = x^3$ are given by $x = pm^2-2qmn+p^2n^2$, where $m^3-3pmn^2+2qn^3 = f$. It is easily seen, that whatever be the index of irregularity, there will always be a finite number of expressions of this sort, giving all the values of x. When $-k = 3a^2 \pm 1$, there are a finite number of others given by the above expressions with $p = 4a^2 \pm 1$, $\pm q = 8a^3 \pm 3a$, since the cubic has then the factor $m \mp 2an$.

We may note that in all cases, the values of m and n furnish us with solutions of our equation.

Thus	k	p	q	m	n	x	y
$f=1$	17,	-2,	3,	-23,	26,	5234,	378661
	24,	-2,	4,	-31,	28,	8158,	736844

Now suppose k is negative and equal to $-8n-3$, $n \neq 0$, then it will be found that the classes $(2n+1, \pm 1, 4)$, produce by triplication the principal class, and these three classes will be the only ones to possess this property if the index of irregularity is not divisible by 3, which of course includes the case of regular determinants. The cubics corresponding to these classes are $(n, \mp 1, -2, 0)$ and $(0, 1, 0, k)$, and are all reducible. Hence there will be a finite number of representations of f by the cubics; and we have the interesting result that the equation

$$y^2-kf^2 = x^3,$$

where

$$k \equiv -3 \bmod 8,$$

negative, and free from square factors, and f is such that x is prime to $2kf$, and also the index of irregularity for proper binary quadratics of

determinant $+k$, $\not\equiv 0 \bmod 3$, has none or limited number of solutions.* The case $n=0$ is no exception, for then there is only one properly primitive class. In particular when $f=1$, the only solutions are when

$$8n+3 = 3a^2 \pm 1, \quad \text{for which} \quad x = 4a^2 \pm 1,$$

or $$8n+3 = 3a^2 \pm 8, \quad ,, \quad x = a^2 \pm 2.$$

Instead of $y^2-kf^2=x^3$, we might have considered $y^2-k=x^3$, where k may have square factors, but is such that x is prime to $2k$. It can be shewn in exactly the same way, that the solution now depends upon the representation of unity, by binary cubics of determinant $4k$.

I have since shewn that the solution of $y^2=x^3+Ax+B$, depends upon the representation of unity by binary quartics with invariants $g_2, g_3 = -4A, -4B$.

14. At present, there is no general method of determining whether or not a given number can be represented by a given binary cubic; but, as before, we can obtain interesting results by considering congruences to various moduli.

Let (F, G, H) be a subtriplicate binary quadratic of determinant k. This class belongs to the principal genus, and hence we can take

$$F \equiv 1 \equiv G \bmod 3.$$

If (a, b, c, d) is the cubic having this for its Hessian, we find if

$$q^2-kp^2 = F^3,$$

$$a \equiv p, \quad b \equiv p+q, \quad c \equiv (k+1)p+2q, \quad d \equiv (1+3k)p+(3+k)q,$$

to mod 9. We may suppose that F is prime to $2kp$, and incapable of representation by the principal class, as the cubic is then reducible, and we can easily see if it supplies us with values of x. Now let $kf^2 \equiv 1 \bmod 3$ in our equation, then $k \equiv 1 \bmod 3$ and $q^2-p^2 \equiv 1 \bmod 3$, whence

$$p \equiv 0 \bmod 3, \quad q \equiv \pm 1 \bmod 9.$$

Taking the positive sign (the negative one leads to the same results), we have from the representation of f by this cubic

$$pm^3+3m^2n+6mn^2+(4p+3+k)n^3 \equiv f \bmod 9.$$

Taking $f \equiv 1 \bmod 3$ (the value $f \equiv -1 \bmod 3$ leads to the same re-

* For application to irregular determinants, see note in *Messenger of Math.*, Dec. 1912.

sults), we find $n \equiv 1 \bmod 3$, whence

$$pm^3+3m^2+6m+4p+3+k \equiv f \bmod 9,$$

or
$$m^2+\tfrac{1}{3}(p+6)m \equiv \tfrac{1}{3}(f-4p-k-3) \bmod 3,$$

and if $p \equiv 0 \bmod 9$, this congruence is impossible if

$$f-k-3 \equiv 3 \bmod 9,$$

or
$$f^3-kf^2 \equiv -3f^2 \bmod 9,$$

or
$$kf^2 \equiv 4 \bmod 9.$$

This applies to all the values of p, and if it holds for all the subtriplicate binary quadratics, our equation $y^2-kf^2 = x^3$ is impossible.

So, if $p \equiv \pm 3 \bmod 9$, the corresponding congruence is impossible if $kf^2 \equiv 7 \bmod 9$.

Similarly, if $F \equiv -1 \bmod 3$, we find $q \equiv 0 \bmod 3$, and that the above results hold if p is replaced by q.

Proceeding similarly with the various values of kf^2, we have the following scheme for impossible equations:—

$kf^2 \equiv 4 \bmod 9$	and	$p \equiv 0 \bmod 9$	(or q if $F \equiv -1 \bmod 3$),
$kf^2 \equiv 7$,,		$p \equiv \pm 3$,,	
$kf^2 \equiv 2$,,		q or $p \equiv 0$,,	
$kf^2 \equiv 5$,,		q or $p \equiv \pm 3$,,	
$kf^2 \equiv -3$,,		$p \not\equiv \pm f$,,	
$kf^2 \equiv 3$,,		$p \equiv 0 \bmod 3$.	

Also $q^2-kp^2 = F^3$, where $F \equiv 1 \bmod 3$, except in the first two cases where we may take $F \equiv -1 \bmod 3$. Further, F is prime to $2kp$. When k is negative, we can take F to be a prime, and there will be only two values for p, differing only in sign. Thus for $k = -29$ and $q^2+29p^2 = 125$, $q = 3$, and for $k = -38$, $q^2+38p^2 = 343$ and $p = 3$, and hence the two equations $y^2-k = x^3$, $-k = 29, 38$ are impossible, as the principal binary quadratic form of determinant $+k$ gives rise to a reducible cubic giving no values of x, and further there are only two irreducible cubics (which are improperly equivalent) arising from two improperly equivalent quadratics.

15. When k is positive, there are an infinite number of values for p. In particular, when the class number is not divisible by 3, we can take F

equal to 1, and hence $q^2-kp^2=1$. If either q or p in the first solution is divisible by 9, this will be the case with every solution, but if q or $p \equiv \pm 3 \mod 9$, this will also be the case with all solutions except those given by

$$q_1+p_1\sqrt{k}=(q+p\sqrt{k})^{3n}.$$

The corresponding cubic, however, belongs to the reducible class, and our scheme will be found to agree with the results of § 9.

When $k \equiv 5 \mod 8$, we have for $kf^2 \equiv 4 \mod 9$, the condition $p \equiv 0 \mod 9$, where q, p is the first solution of $q^2-kp^2=1$. But since the class number is not divisible by 3, T and U are both odd in the first solution of $T^2-kU^2=4$, and we have the relation

$$q+p\sqrt{k}=\tfrac{1}{8}(T+U\sqrt{k})^3.$$

Hence $8p=U(3T^2+kU^2)$, but $U \equiv 0 \mod 3$, and hence

$$p \equiv 0 \mod 9,$$

so that our equation $y^2-kf^2=x^3$ is impossible. It is easily seen that a similar result holds when $kf^2 \equiv 2, \pm 3 \mod 9$.

16. As before we can obtain some results by considering congruences to mod 7. Thus, let (F, G, H) be the Hessian, where we may take $F \equiv 1, 2$ or $4 \mod 7$ and $G \equiv 1 \mod 7$. Then for the representation of f by the corresponding cubic, we have

$$(Fm+Gn+n\sqrt{k})^3(q+p\sqrt{k})-(Fm+Gn-n\sqrt{k})^3(q-p\sqrt{k})=2F^3f\sqrt{k},$$

where

$$q^2-kp^2=F^3.$$

If $kf^2 \equiv 4 \mod 7$, then since $F^3 \equiv 1 \mod 7$, $kp^2 \equiv 0, 1 \mod 7$, and we can shew that if $p \equiv 0 \mod 7$, our equation is impossible. For then $q \equiv \pm 1 \mod 7$, $f\sqrt{k} \equiv \pm 2 \mod 7$, and hence the above equation can be written $P^3+Q^3 \equiv 4 \mod 7$, which is impossible.

If k is positive, we may take $F=1$, and if in the first solution $p \equiv 0 \mod 7$, this will be true for all the values of p, and our equation is impossible. In particular if $k \equiv 5 \mod 8$, then since the class number is supposed not divisible by 3, we have for the first solution p, q,

$$8p=U(3T^2+kU^2),$$

where T, U is the first solution of

$$T^2-kU^2=4.$$

But since $kf^2 \equiv 4 \mod 7$, we find either $U \equiv 0 \mod 7$, or $U \equiv \pm f$, $T \equiv \pm 1 \mod 7$, and in both cases $p \equiv 0 \mod 7$, and the equation is insoluble.

17. We can now draw up a scheme, giving the values of k between ± 100 for which $y^2-k=x^3$ is soluble or not. Thus, for

$$-k = 7, 15, 18, 20, 23, 25, 26, 28, 39, 40, 45, 47, 48, 53, 54, 55, 56, 60,$$
$$61, 63, 71, 72, 79, 83, 87, 89, 95, 100,$$

there are, I believe, an infinite number of solutions. For the other values of $-k$ between 1 and 100 there are none or a finite number of solutions, except when $-k = 31, 84$, and in these cases, whether or not the equations are insoluble I cannot say. When

$$k = 1, 4, 6, 7, 11, 13, 14, 16, 20, 21, 23, 25, 27, 29, 32, 34, 39, 42, 45,$$
$$46, 47, 49, 51, 53, 58, 59, 60, 61, 62, 66, 67, 69, 70, 75, 77, 78,$$
$$83, 84, 85, 86, 87, 88, 90, 93, 95, 96,$$

the equations are insoluble or admit only a limited number of solutions. For the remaining values of k, there are an infinite number of solutions, except when $k = 74$, in which case nothing can be said about the equation. When k is a perfect square, we may note that the solution* of $y^2 = x^3+k$ involves that of $x^3+y^3 = 2\sqrt{k}$ and *vice versa*. We have made use of this when $k = 1, 4, \ldots$.

I take this opportunity of acknowledging my great indebtedness to the referees who have suggested many improvements.

* Due to Lucas, I believe, *Nouvelles Annales*, 1878, p. 425.