THE RATIONAL SOLUTIONS OF THE DIOPHANTINE EQUATION. $Y^2 = X^3 - D$.

By

J. W. S. CASSELS

TRINITY COLLEGE, CAMBRIDGE.

1. We study the rational solutions X, Y of the equation

$$Y^2 = X^3 - D \tag{1}$$

where D is a given integer, a problem of a type considered by Bachet over three centuries ago. When $D = \pm 1$ Euler[1] [10] showed that the only solutions are $X = 2$, $Y = \pm 3$ and trivial ones with $X = 0$ or $Y = 0$. Apart from a treatment of the special case when D is a perfect cube by Nagell [29], the first significant advance for many years was made by Fueter [12] who writes the equation as

$$X^3 = Y^2 + D\,,$$

assumes that $D > 0$, and studies factorisation in $R(\sqrt{(-D)})$. This work has been extended by Brunner in a doctorate thesis [3]. The case $D < 0$ was considered by Mordell [26] and then by Chang Kuo-Lung [5].

2. The integral solution ξ, η, ζ of the equation

$$\xi^3 + \eta^3 = A\zeta^3\,, \qquad (\zeta \neq 0)$$

where A is a given integer, is trivially equivalent to the rational solution of (1) with $D = 2^4 3^3 A^2$ by putting

$$X : Y : A = 2^2 3 \zeta : 2^2 3^2 (\xi - \eta) : \xi + \eta\,.$$

The case $A = 1$ is, of course, Fermat's problem with exponent 3. The equation with general A was extensively investigated in the 19th Century by Lucas [19], Pépin [36, 37] and Sylvester [40]; and Sylvester states that he either had a solution or

[1] For references see end of paper.

knew the equation to be insoluble for all positive $A < 100$ except[1] $A = 66$. Further results have been given by Hurwitz [17], Faddeev [11] and Holzer [16]. Much of this work is summarized by Nagell [31]. [added in the proof]. Since this was written new and interesting work has been done by Dr. E. S. Selmer (so far unpublished).

3. The equation (1) is, of course, a special case of

$$Y^2 = X^3 - CX - D \tag{2}$$

where C and D are integers. This was studied by Poincaré [38] who noted that the values of the parameter u corresponding to rational solutions form an additive group, $\mathfrak{U}$, when the usual parametrization $Y = \frac{1}{2}\wp'(u)$, $X = \wp(u)$ is employed. This group was shown to have a finite basis by Mordell [25]. A more precise form of this result was given by Weil (cf. theorem II) who gives an elementary proof [42] as well as a deep proof of a far-reaching generalization [41]. In a doctorate thesis, Billing [2] has given a general study of (2) using methods based on Weil's theorem and, in particular, he gives a complete solution of (1) for all $|D| \leq 25$ in the sense that he gives a complete basis for $\mathfrak{U}$. He does not, however, give a detailed account of the method of obtaining these results. The present work was done in ignorance of Billing's paper; indeed, it was not until a late stage that I realized that the algorithm which I employed was that underlying Weil's theorem II. In it, I have developed a more detailed theory of (1) than is given by Billing and have given general theorems as well as carrying the solution up to $|D| \leq 50$. With one exception ($D = -15$), my results confirm Billing's in the range $|D| \leq 25$ studied by him. I have been led to compute a table[2] of class-numbers and units for all cubic fields $R(\sqrt[3]{D})$ with $|D| \leq 50$; which I do not think has been given before, although a number of partial tables exist. Finally, it should be remarked that (2) is the subject of a series of papers by Nagell [30, 32, 34, 35] and that other aspects of the problem have been studied by Châtelet [6, 7], Lutz [20] and Lind [18].

4. In part I, I give a resumé of the general theory of (2) and discuss its relevance to (1) in general terms. In part II the general discussion is carried further using the specific arithmetical properties of the relevant cubic number-fields, and in part III the actual applications are made.

[1] Insoluble by theorem VIII.

[2] Table 2.

Part I.

5. Let (X', Y') and (X'', Y'') be any two rational solutions[1] of $Y^2 = X^3 - CX - D$ with parameters u', u'' and let (X''', Y''') be the solution with parameter $u''' = u' + u''$. Then (X', Y'), (X'', Y'') and $(X''', -Y''')$ lie on a straight line $y = Ax + B$ by a known result[2], where A and B must be rational. Hence X', X'', X''' are the roots of

$$X^3 - CX - D - (AX+B)^2 = 0\,. \tag{3}$$

The left-hand side of (3) must be identical with $(X-X')(X-X'')(X-X''')$ and so, if δ is a root of $\delta^3 - C\delta - D = 0$,

$$(X'-\delta)(X''-\delta)(X'''-\delta) = (A\delta+B)^2\,,$$

i. e.

$$(X'''-\delta) = (X'-\delta)(X''-\delta)\beta^2,\ \beta \in R(\delta)\,. \tag{4}$$

In other words, if squared factors are ignored, the values of $X - \delta$ form a multiplicative group homomorphic to $\mathfrak{U}$. There are three groups $\mathfrak{G}_1$, $\mathfrak{G}_2$, $\mathfrak{G}_3$ (say) corresponding in this way to the three values δ_1, δ_2, δ_3 (say) of δ. If $\delta^3 - C\delta - D$ is irreducible, the numbers $X - \delta_j$ $(j = 1, 2, 3)$ are conjugate algebraic numbers, and the three groups $\mathfrak{G}_j$ run entirely parallel to one another. If, however, $\delta^3 - C\delta - D$ is reducible, this parallelism does not necessarily hold and so we are compelled to introduce a group $\mathfrak{G}$ in terms of "triplets".

A triplet $\{\alpha_j\}$ is defined as a set of three numbers $\alpha_1, \alpha_2, \alpha_3$ such that $\alpha_j \in R(\delta_j)$ and the operations of addition and multiplication for triplets are defined by

$$\{\alpha_j\} + \{\beta_j\} = \{\alpha_j + \beta_j\}\,;\quad \{\alpha_j\}\{\beta_j\} = \{\alpha_j\beta_j\}\,.$$

Then the set of triplets $\{X - \delta_j\}$ is clearly also a multiplicative group $\mathfrak{G}$ homomorphic to $\mathfrak{U}$, when squared (triplet) factors are ignored. Obviously, when $\delta^3 - C\delta - D$ is *irreducible* $\mathfrak{G}$ is isomorphic to each of the groups $\mathfrak{G}_j$.

We denote, further, by $2\mathfrak{U}$ the set of $2u$, $u \in \mathfrak{U}$. Clearly $2\mathfrak{U}$ forms a group. We denote the quotient group of $\mathfrak{U}$ and $2\mathfrak{U}$ by $\mathfrak{U}/(2\mathfrak{U})$. Then the following three theorems hold.

Theorem I (Mordell). *The group* $\mathfrak{U}$ *has a finite basis.*

Theorem II (Weil). $\mathfrak{G}$ *is isomorphic to* $\mathfrak{U}/(2\mathfrak{U})$. *The element of* $\mathfrak{G}$ *and the element*

[1] (X, Y) (with or without affixes) will always be a rational solution of $Y^2 = X^3 - CX - D$.

[2] cf. Whittaker and Watson [44].

of $\mathfrak{U}/(2\mathfrak{U})$ *belonging to the same solution of* $Y^2 = X^3-CX-D$ *correspond to one another in the isomorphism.*

Theorem III. *Let* (I) w *be the number of independent generators of infinite order in* $\mathfrak{U}$, (II) g *be the number of generators of* $\mathfrak{G}$ *and* (III) $s=0, 1, 2$ *according as* $\delta^3-C\delta-D=0$ *has no, has one or has three rational solutions. Then* $w = g-s$.

Theorem III is really a corollary of theorem II. For proofs we refer to the paper of Weil [42] or the book of Delaunay and Faddeev [9].

6. If $\mathfrak{G}$ is known, then, by theorems II and III, the structure of $\mathfrak{U}$ is known, except for its generators of finite order. A theorem has been given by Lutz [21] which, while not completely characterizing the solutions of finite order of $Y^2 = X^3-CX-D$ (i. e. those solutions whose parameters are of finite order in $\mathfrak{U}$), reduces the problem, when C and D are given, to the study of a manageable number of cases. We shall not need it here, but quote it for completeness.

Theorem IV (Lutz). *If* X, Y *is a rational solution of* $Y^2 = X^3-CX-D$ *of finite order, then* X *and* Y *are integers and* $Y^2/(4C^3-27D^2)$.

This is superseded in the case $C = 0$ by

Theorem V (Fueter-Billing). *Solutions of* $Y^2 = X^3-D$ *with* $X = 0$ or $Y = 0$ *are of order* 3 *and* 2 *respectively. The only other solutions of finite order are the two following:—*

$$X = 2,\ Y = \pm 3,\ D = -1\,; \tag{5}$$

$$X = 2^2 3,\ Y = \pm 2^2 3^2,\ D = 2^4 3^3\,; \tag{6}$$

of order 6 *and* 3 *respectively.*

7. Another general theorem is

Theorem VI (Fueter-Billing). *The number* w^* *(say) of independent generators of infinite order of the group* $\mathfrak{U}^*$ *(say) of the equation* $Y^2 = X^3+27D$ *is equal to the corresponding number* w *for* $Y^2 = X^3-D$.

The interdependence between these two equations has been known for a long time. It is connected with the possibility of "complex multiplication" of the parameter u by $\surd(-3)$.

8. Finally, we enunciate the almost trivial

Theorem VII. *There is a* $1-1$ *correspondence between the rational solutions* X, Y *of* $Y^2 = X^3-CX-D$ *and the integer solutions* x, y, t *of*

$$y^2 = x^3 - Cxt^4 - Dt^6,\ t > 0,\ (x, t) = (y, t) = 1\ . \tag{7}$$

This follows immediately by putting $X = x/r$, $Y = y/s$ where x, y, r, s are integers and the fractions are in their lowest terms. Comparison of denominators on both sides of $Y^2 = X^3 - CX - D$ gives $s^2 = r^3$ and hence $s = t^3$, $r = t^2$ for some t. It will be more convenient to use this form in future. We note that the multiplicative group $\mathfrak{G}$ of the triplets $\{X - \delta_j\}$ may also be defined as the group of the $\{x - t^2\delta_j\}$, squared factors again being ignored.

Part II.

9. We shall now confine ourselves to the equation

$$y^2 = x^3 - Dt^6,\ t \neq 0,\ (x, t) = (y, t) = 1\ , \tag{8}$$

where x, y, t are integers. We may clearly assume that D is sixth-power-free and, by theorem VI that $27 \nmid D$. Any such D can be put in the form[1]

$$D = EF^2G^3,\ E > 0,\ F > 0,\ 3 \nmid G\ , \tag{9}$$

$$(E, F) = 1\ , \tag{10}$$

$$E, F, G \text{ squarefree}\ . \tag{11}$$

By theorems III and V the structure of the group $\mathfrak{U}$ of solutions can be found from that of the group $\mathfrak{G}$. Until further notice, we shall assume that D is not a perfect cube and so, by theorem III, the number of independent generators of infinite order of $\mathfrak{U}$ is equal to the number of generators of $\mathfrak{G}$. Further, all three expressions $x - t^2\delta_j$ $(j = 1, 2, 3)$ where δ_j runs through the roots of $\delta^3 = D$, are conjugate, and so we need study only one, say $x - t^2\delta$ where δ is the real cube root of D. We first state some properties of the cubic fields $R(\delta)$. For proofs see a paper by Dedekind [8] or the general theory in Weyl [43].

10. Write

$$\delta = G\Delta,\ D^* = EF^2 = \Delta^3 > 1\ .$$

Small Greek letters denote numbers in $R(\Delta)$, Gothic small letters denote ideals, as also do square brackets enclosing a (possibly redundant) basis. If $D^* \not\equiv \pm 1 \bmod 9$ integers in $R(\Delta)$ have the basis $\{1, \Delta, \Delta^2/F\}$ but if $D^* \equiv \pm 1 \bmod 9$ the basis is $\{1, \Delta, \Delta^2/F, \frac{1}{3}(1 \pm \Delta + \Delta^2)\}$. In particular

[1] For let $p^s // D$ where p is a rational prime. According as $s = 1, 2, 3, 4, 5$ we make $(s = 1)$ $p // E, p \nmid FG$; $(s = 2)$ $p // F, p \nmid EG$; $(s = 3)$ $p // G, p \nmid EF$; $(s = 4)$ $p // E, p \nmid F, p // G$; $(s = 5)$ $p \nmid E, p // F, p // G$. Further, sign G = sign D.

Lemma 1. *The number $a+b\varDelta$, where a and b are rational, is an integer in $R(\varDelta)$ if and only if a and b are integers.*

The rational primes p factorise as follows in $R(\varDelta)$:

p/D^*: $p = \mathfrak{p}^3$ where $\mathfrak{p} = [p, \varDelta]$ or $\mathfrak{p} = [p, \varDelta^2/F]$ according as p/E or p/F.

$p = 3\nmid D^*$, $D^* \not\equiv \pm 1 \bmod 9$: $3 = \mathfrak{r}^3$, $\mathfrak{r} = [3, \mp\varDelta]$ where $D^* \equiv \pm 1 \bmod 3$.

$p = 3\nmid D^*$, $D^* \equiv \pm 1 \bmod 9$: $3 = \mathfrak{r}^2\mathfrak{s}$ where
$\mathfrak{r} \doteq [3, 1\mp\varDelta, \tfrac{1}{3}(1\pm\varDelta+\varDelta^2)]$,
$\mathfrak{s} = [3, 1\mp\varDelta, \tfrac{1}{3}(-2\pm\varDelta+\varDelta^2)]$.
Here $\mathfrak{r}\mathfrak{s} = [3, 1\mp\varDelta]$.

$p \equiv -1 \bmod 3$, $p\nmid D^*$: $p = \mathfrak{p}\mathfrak{q}$ where
$\mathfrak{p} = [p, d-\varDelta]$,
$\mathfrak{q} = [p, d^2+d\varDelta+\varDelta^2]$
and d is the unique root of the congruence $d^3 \equiv D^* \bmod p$.
$\mathfrak{p}$ and $\mathfrak{q}$ are of the first and second degrees respectively.[1]

$p \equiv 1 \bmod 3$, $p\nmid D^*$, D^* a cubic residue of p: $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ where $\mathfrak{p}_j = [p, d_j-\varDelta]$ and d_1, d_2, d_3 are the distinct roots of $d^3 \equiv D^* \bmod p$.

$p \equiv 1 \bmod 3$, $p\nmid D^*$, D^* not a cubic residue of p: p remains prime in $R(\varDelta)$.

The following are quoted for reference as lemmas. The proofs are elementary.

Lemma 2. *Let a, b be rational integers and $p\nmid(a, b)$ a rational prime. Suppose $p \neq 3$ if $D^* \equiv \pm 1 \bmod 9$. Then either p is prime to $a+b\varDelta$ or*

$$[p, a+b\varDelta] = \mathfrak{p}^w$$

where $\mathfrak{p}$ is some first degree prime divisor of p.

Lemma 3. *If $\mathfrak{p}$ is a prime ideal of the first degree the rational integers $0, 1, 2, \ldots, p-1$ are a complete set of incongruent residues* mod $\mathfrak{p}$ *where* $p =$ Norm $\mathfrak{p}$.

Lemma 4. *If $\mathfrak{q}$ is a prime ideal of the second degree the numbers*

$$a+b\varDelta \quad (a, b = 0, 1, 2, \ldots, p-1)$$

are a complete set of incongruent residues mod $\mathfrak{q}$ *where* $p^2 =$ Norm $\mathfrak{q}$.

Lemma 5. *Let $\mathfrak{t}$ be a prime ideal and $\mathfrak{t}^s/2$ for some $s > 0$. Then $\alpha \equiv \beta$* mod $\mathfrak{t}^s$

[1] i. e. Norm $\mathfrak{p} = p$, Norm $\mathfrak{q} = p^2$.

implies $\alpha^2 \equiv \beta^2 \bmod \mathfrak{t}^{2s}$. *Indeed it implies* $\alpha^2 \equiv \beta^2 \bmod \mathfrak{t}^{2s+1}$ *if* $\mathfrak{t}$ *is of the first degree. In particular* $\alpha^2 \equiv 1 \bmod \mathfrak{t}^3$ *if* $\mathfrak{t}$ *is of the first degree and* $\mathfrak{t} \nmid \alpha$.

11. The units of $R(\Delta)$ are all of the form $\pm\varepsilon^n$ where $\varepsilon > 0$ is the fundamental unit. For our present purpose it is enough to know any odd power[1] $\eta = \varepsilon^{2n+1} > 0$ of ε. Values of η and of the classnumber h of $R(\Delta)$ are given in table 2. As a special case of a known general theorem we have[2]

Lemma 6. *If h is odd, η is not a quadratic residue of* 4.

Let now $\mathcal{H}$ be the principal class of ideals in $R(\Delta)$ and $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_k$ the classes of order 2, if any, i.e. $\mathcal{C}_j \neq \mathcal{H}$, $\mathcal{C}_j^2 = \mathcal{H}$. Let $\mathfrak{c}_j \in \mathcal{C}_j$ and choose $\gamma_j > 0$ such that $[\gamma_j] = \mathfrak{c}_j^2$. Then every number $\theta > 0$ of $R(\Delta)$ for which $[\theta]$ is the square of an ideal has one of the forms

$$\alpha^2, \ \eta\alpha^2, \ \gamma_j\alpha^2, \ \eta\gamma_j\alpha^2 .$$

The γ_j can be chosen to be integers prime to any given ideal $\mathfrak{m}$. Hence, if θ is an integer, α contains in its denominator only ideals prime to $\mathfrak{m}$. In particular, we shall suppose henceforth that the γ_j are prime to 2. There is a generalisation of lemma 5 which states that then precisely half of the numbers

$$1, \eta, \gamma_j, \eta\gamma_j \qquad (j = 1, 2, \ldots, k)$$

are quadratic residues of 4. We shall not use this generalisation in the general theory but in numerical work we shall use the corollary that if η is not a quadratic residue of 4 the γ_j may be chosen all to be quadratic residues, to give a normalisation of the γ_j where possible. This is always possible in the range $|D| \leq 50$, since there η is not a quadratic residue of 4.

12. Consider the factorisation

$$y^2 = (x - Gt^2\Delta)(x^2 + Gt^2x\Delta + G^2t^4\Delta^2) .$$

[1] It is difficult to decide if a given unit $\eta_1 > 0$ is a fundamental unit but easy to decide if it is a perfect square. If not, put $\eta = \eta_1$.

[2] Lemma 6 belongs to the general theory of class-fields as expounded by Hasse [13, 14]. The full force of this theory is not required and it is possible to base a proof on the simpler theory of relative-quadratic fields developed by Hilbert [15]. By Satz 4 on page 374 of [15] if η is a quadratic residue of 4, the relative-discriminant of $R(\Delta, \sqrt{\eta})$ over $R(\Delta)$ is unity, since it has no prime factors. By Satz 94 on page 155 (and the remark on page 156 extending it to $l = 2$ in the there notation if a further condition is satisfied) it follows that h is even.

In the language of class-field theory if η is a quadratic residue of 4 the field $R(\Delta, \sqrt{\eta})$ is unramified (*unverzweigt*) over $R(\Delta)$ and so is the class-field to some absolute ideal group of index 2. This implies that h is even.

Any common divisor $\mathfrak{a}$ of the two terms on the right hand side must divide

$$x^2+Gt^2x\Delta+G^2t^4\Delta^2-(x-Gt^2\Delta)^2 = 3Gt^2x\Delta$$

and so $\mathfrak{a}/3G\Delta$ since $(x, t) = 1$. Hence $[x-Gt^2\Delta] = \mathfrak{a}\mathfrak{b}^2$ for some ideal $\mathfrak{b}$ and $\mathfrak{a}/3G\Delta$. We classify the prime divisors of $\mathfrak{a}$ as follows

(*i*) $\mathfrak{p}/\Delta$. Then $\mathfrak{p}^3 = [p]$ where $p = \text{Norm } \mathfrak{p}$. Since p occurs in $y^2 = \text{Norm } (x-Gt^2\Delta)$ to an even power, $\mathfrak{p}$ occurs in $x-Gt^2\Delta$ to an even power, and so may be absorbed in $\mathfrak{b}$.

(*ii*) $\mathfrak{q}/G$ but $\mathfrak{q}\nmid\Delta$, so $\mathfrak{q}\nmid 3$ by (9). Then $\mathfrak{q}/x$ since $\mathfrak{q}/G$ and $\mathfrak{q}/(x-Gt^2\Delta)$ i. e. q/x where q is the rational prime divisible by $\mathfrak{q}$. Write $x = qx_1$, $G = qG_1$. By lemma 2, either $x_1-G_1t^2\Delta$ is prime to q or $[q, x_1-G_1t^2\Delta] = \mathfrak{q}'^w$ for *some* first degree prime divisor $\mathfrak{q}'$ of q, since $q\nmid G_1t^2$ [as $q\nmid G_1$ by (11) and $q\nmid t$ by (8) (and q/x)]. But $y^2 = \text{Norm } (x-Gt^2\Delta) = q^3 \text{Norm } (x_1-G_1t^2\Delta)$ and so the second alternative holds and $\mathfrak{q}'$ divides $x_1^2-G_1t^2\Delta$ to an odd power.

(*iii*) $\mathfrak{p}/3$ but $\mathfrak{p}\nmid G\Delta$. Hence $3\nmid D$ but $3/y$ since $y^2 = \text{Norm } (x-Gt^2\Delta)$. Consequently $x^3 \equiv G^3t^6D^*$ mod 9 so this case occurs only when $D^* \equiv \pm 1$ mod 9 i. e. when $[3] = \mathfrak{r}^2\mathfrak{s}$. Now $x^3 \equiv G^3t^6D^* \equiv \pm G^3t^6$ mod 9 implies $x \equiv \pm Gt^2$ mod 3 and so $\mathfrak{r}\mathfrak{s}/(x-Gt^2\Delta)$ since $\mathfrak{r}\mathfrak{s} = [3, 1\mp\Delta]$. But $3\nmid(x-Gt^2\Delta)$ (lemma 1) so $\mathfrak{r}//(x-Gt^2\Delta)$. Hence $\mathfrak{s}$ occurs in $x-Gt^2\Delta$ to an odd power since $y^2 = \text{Norm } (x-Gt^2\Delta)$ and $\text{Norm } \mathfrak{r} = \text{Norm } \mathfrak{s} = 3$.

All this proves

Lemma 7. *Let $q_1, \ldots, q_l$ be the rational primes such that $q_j/(x, G)$ but $q_j\nmid D^*$. Then*

$$[x-Gt^2\Delta] = \frac{q_1}{\mathfrak{q}_1} \cdot \ldots \cdot \frac{q_l}{\mathfrak{q}_l} \cdot \mathfrak{b}^2, \tag{12}$$

where $\mathfrak{q}_j$ is some first degree prime divisor of q_j and $\mathfrak{b}$ is some ideal; except that, when $D^* \equiv \pm 1$ mod 9 and $3/y$,

$$[x-Gt^2\Delta] = \frac{q_1}{\mathfrak{q}_1} \cdot \ldots \cdot \frac{q_l}{\mathfrak{q}_l} \cdot \mathfrak{r}\mathfrak{s} \cdot \mathfrak{b}^2. \tag{13}$$

In particular $[x-Gt^2\Delta] = \mathfrak{a}\mathfrak{b}^2$ where $\mathfrak{a}$ is one of a finite set. Hence $\mathcal{H} = \mathcal{A}\mathcal{B}^2$ where $\mathcal{A}$ and $\mathcal{B}$ are the ideal classes to which $\mathfrak{a}$ and $\mathfrak{b}$ belong and $\mathcal{H}$ (as before) is the principal class. For given $\mathfrak{a}$ and so for given $\mathcal{A}$, this equation for $\mathcal{B}$ may be insoluble (e.g. when[1] the class-number $h = 2$ and $\mathscr{A} \neq \mathscr{H}$). If however $\mathscr{A}\mathscr{B}^2 = \mathscr{H}$ has the solution $\mathscr{B} = \mathscr{B}_1$, the other solutions are all the $\mathscr{B} = \mathscr{B}_1 \mathscr{b}_j$ where $\mathscr{b}_j$ (as before) runs through all the solutions of $\mathscr{b}^2 = \mathscr{H}$, $\mathscr{b} \neq \mathscr{H}$. We may choose $\mathfrak{b}_1 \in \mathscr{B}_1$ and prime to any given ideal $\mathfrak{m}$. Then $\mathfrak{a}\mathfrak{b}_1^2$ is a principal ideal, say $\mathfrak{a}\mathfrak{b}_1^2 = [\lambda]$. Now $[x - Gt^2\Delta] = \mathfrak{a}\mathfrak{b}^2 = [\mathfrak{a}\mathfrak{b}_1^2][\mathfrak{b}\mathfrak{b}_1^{-1}]^2$ where $\mathfrak{b}\mathfrak{b}_1^{-1} \in \mathscr{B}\mathscr{B}_1^{-1} = \mathscr{b}_j$ for some j, or $= \mathscr{H}$.

Hence finally

$$x - Gt^2\Delta = \pm\lambda\alpha^2 \text{ or } \pm\eta\lambda\alpha^2 \text{ or } \pm\gamma_j\lambda\alpha^2 \text{ or } \pm\eta\gamma_j\lambda\alpha^2\,,$$

say

$$x - Gt^2\Delta = \mu\alpha^2 \tag{14}$$

where μ is an integer in $R(\Delta)$ taken from a finite set, which may be chosen so that α, though not necessarily an integer, has in its denominator only factors prime to any given[2] $\mathfrak{m}$. We note that $\mu > 0$ since $x^3 - (Gt^2\Delta)^3 = y^2 > 0$.

We shall say that two values of μ are *essentially similar* if their quotient is a square in $R(\Delta)$, otherwise *essentially dissimilar*. The values of μ which actually correspond to solutions of (8) form the multiplicative group $\mathfrak{G}$, when squared factors are ignored, which we discussed earlier. We shall use this group-property frequently. We note in particular that we can assume that μ is essentially distinct from 1 when investigating the number of generators of $\mathfrak{G}$. As we remarked earlier, the number of generators of $\mathfrak{G}$ is the number of generators of infinite order of $\mathfrak{U}$.

13. All the argument so far applies equally to the equation $y^2 = x^3 + Dt^6$ in which the sign of D is changed and leads to the equation

$$x + Gt^2\Delta = \mu\alpha^2 \tag{15}$$

in which μ has the same *a priori*[3] possible values as for (14). It will often be convenient to discuss (14) and (15) simultaneously and then, in numerical work, we shall always mean by D, δ the *positive* values and make the appropriate changes in the formulae when discussing negative D. General theorems will, however, apply equally to either positive or negative D.

[1] A numerical case is $D = \pm 88$ and $2/x$. Then $G = 2$, $D^* = 11$, $h = 2$ and $\mathfrak{a} = \mathfrak{u}$ is the second-degree divisor of [2] in $R(\sqrt[3]{11})$, which is not a principal ideal. Hence there are no solutions with $D = \pm 88$, $2/x$ [indeed none with $D = \pm 88$ at all]. A similar argument in a quadratic field has been used by Mordell and independently by Marshall Hall (both unpublished).

[2] We require only $\mathfrak{m} = 6$.

[3] i. e. so far as the discussion in part II is concerned. We shall use *a priori* in this sense throughout part III.

Part III.

14. In this part we give a number of general theorems covering most of the values of D such that $|D| \leq 50$ and then dispose of the rest individually.

15. *D odd.* We examine (14) modulo powers of $\mathfrak{t}$ and $\mathfrak{u}$, the prime divisors of $[2]$ of the first and second degrees respectively. We note that

$$\mathfrak{t} = [2, 1+\delta], \mathfrak{t}^2 = [4, D-\delta], \mathfrak{t}^3 = [8, D-\delta] ,$$

$$\mathfrak{u} = [2, 1+\delta+\delta^2], \mathfrak{u}^2 = [4, 1+D\delta+\delta^2], \mathfrak{u}^3 = [8, 1+D\delta+\delta^2] .$$

We prove first

Theorem VIII. *If D is odd and* (14) *is true then either μ is a quadratic residue of* 4 *or*

$$\mu \equiv D-\delta, 2-\delta, D-2\delta \qquad \text{mod } \mathfrak{u}^2 . \tag{16}$$

One and only one of x, y, t is even since $(x, t) = (y, t) = 1$ and we take the possibilities in turn.

(*i*) *t even.* Then $x \equiv x^3 \equiv y^2 \equiv 1$ mod 8 so $\mu\alpha^2 = x-t^2\delta \equiv 1$ mod 4 and μ is a quadratic residue of 4.

(*ii*) *y even.* Then $x \equiv x^3 \equiv Dt^6 \equiv D$ mod 4 and so $\mu\alpha^2 = x-t^2\delta \equiv D-\delta$ mod 4. But α is prime to $\mathfrak{u}$ since $x-t^2\delta$ is (by lemma 2). Hence

$$\mu = (x-t^2\delta)(1/\alpha)^2 \equiv (D-\delta)(1/\alpha)^2 \qquad \text{mod } \mathfrak{u}^2 .$$

By lemma 4, $(1/\alpha) \equiv 1, \delta, 1+\delta$ mod $\mathfrak{u}$ so, by lemma 5, $(1/\alpha)^2 \equiv 1^2, \delta^2, (1+\delta)^2$ mod $\mathfrak{u}^2$ and then (16) holds.

(*iii*) *x even.* Then $D \equiv Dt^6 \equiv -y^2 \equiv -1$ mod 8. If $4/x$, then $\mu\alpha^2 = x-t^2\delta \equiv -\delta \equiv (\delta^2)^2$ mod 4 so μ is a quadratic residue of 4. If, however, $2//x$ then $\mu\alpha^2 = x-t^2\delta \equiv 2-\delta$ mod 4 and so (16) holds.

This concludes the proof.

Corollary 1. *If D is odd and μ is not a quadratic residue of* 4 *at least one of* (14) *or* (15) *is insoluble.*

For if (16) is true the corresponding congruences in which the signs of D and δ are simultaneously changed cannot be true.

In particular,

Corollary 2. *If $D \not\equiv \pm 1$ mod 9 is odd and cube-free*[1] *and if h_D is odd, non-*

[1] It is enough that there is no prime p with $p^3//D$.

trivial solutions do not exist for both $y^2 = x^3 \pm Dt^6$. If non-trivial solutions do exist for one of these equations then the corresponding group $\mathfrak{U}$ has precisely one generator of infinite order.

For under the conditions of corollary 2 the only *a priori* possible value of μ essentially dissimilar from 1 is $\mu = \eta$, which is not a quadratic residue of 4 by lemma 6. Hence $\mathfrak{G}$ has at most one generator, i. e. $\mathfrak{U}$ has at most one generator of infinite order (theorem III) and, by corollary 1, such a generator exists for at most one of the two equations. Finally, by theorem V, the only solutions of finite order for the D under consideration are trivial.

We now consider some numerical examples.

Non-trivial solutions actually exist (table 1) for the following values of D for which h_D is odd (table 2) and which satisfy the other conditions of corollary 2:

$$D = -3,\ -5,\ +7,\ -9,\ +13,\ +21,\ +23,\ +25,\ +29,\ -31,\ -33,\ -41,\ +45,\ +49\,.$$

Hence $\mathfrak{U}$ has one generator of infinite order for these D whereas there are no non-trivial solutions at all for

$$D = +3,\ +5,\ -7,\ +9,\ \text{etc.}$$

Consider now $D \not\equiv \pm 1 \bmod 9$ and cube-free, but with h_D even. Then the only possible values of μ essentially different from 1 are $\mu = \eta,\ \gamma_j,\ \eta\gamma_j$. Suppose further that $|D| \leq 50$. Then (table 2) the group of ideal-classes is cyclic, so essentially only one value of $\gamma_j = \gamma$ exists, and γ is a quadratic residue of 4 but η and $\eta\gamma$ are not. As the values of μ for which (14) is soluble form the multiplicative group $\mathfrak{G}$, the group $\mathfrak{U}$ has no, one or two generators of infinite order according as none, or one or all three possible values of μ essentially dissimilar from 1 do in fact have solutions in (14).

In particular, consider $D = +11$. Neither of the solutions $(x, y, t) = (3, 4, 1)$ or $(15, 58, 1)$ leads to a value of μ which is a quadratic residue of 4 (as in the proof of theorem VIII) nor do they belong to the same μ since the ratio

$$(3-\delta)/(15-\delta)$$

is not a perfect square[1]. Hence solutions exist both for $\mu = \eta$ and for $\mu = \eta\gamma$, so also for $\mu = \gamma$ by the group-property of μ. The corresponding group $\mathfrak{U}_{11}$ has thus two generators of infinite order. By corollary 1 there are then no solutions for $D = -11$ either with $\mu = \eta$ or $\mu = \eta\gamma$, so when $D = -11$ the only possible value for μ essentially dissimilar from 1 is $\mu = \gamma$ i. e. the group $\mathfrak{U}_{-11}$ can have at most one

[1] It is not a quadratic residue mod $[5, \delta - 1]$, the first-degree prime divisor of 5.

generator of infinite order. It has precisely one such generator since non-trivial solutions do in fact exist. However $\mu = 1$ or $\mu = \gamma$ is a quadratic residue of 4 for all these solutions and hence so is[1] $x+t^2\delta$. Since $-11 \equiv -1 \bmod 8$, this implies $2/t$, as in the proof of theorem VIII. In particular $X = x/t^2$ and $Y = y/t^3$ cannot be *integers*. The solution given in table 1 for $D = -11$, namely $(x, y, t) = (-7, 19, 2)$ corresponds to[1] $x+t^2\delta = \gamma\alpha^2$ and not to $x+t^2\delta = \alpha^2$ since $-7+4\delta \equiv 5 \bmod \mathfrak{t}^3$ but $\alpha^2 \equiv 1 \bmod \mathfrak{t}^3$ by lemma 5.

Similar arguments apply to $D = \pm 39, \pm 43, \pm 47.$ The only modification necessary when $D = \pm 15$ is that although we can prove that, when $D = +15$, $x-t^2\delta$ is a quadratic residue of 4 this does *not* imply $2/t$ since $15 \equiv -1 \bmod 8$ and we may have $4/x$ as in the case (*iii*) of the proof of the theorem. This in fact does occur.

We leave for later consideration the cases $D \equiv \pm 1 \bmod 9$.

16. We may strengthen theorem VIII somewhat by considering congruences to powers of $\mathfrak{t}$ as well as to powers of $\mathfrak{u}$. We prove the strengthened form although it is not required to deal with $|D| \leq 50$. We require first

Lemma 8. *If D is odd and* (14) *is true but μ is not a quadratic residue of* 4 *then either $2/y$ or $2//x$, the second case occurring only when $D \equiv -1 \bmod 8$. Further $\mu \equiv 3 \bmod \mathfrak{t}^2$ and $\mu \equiv 7$ or $\equiv 3 \bmod \mathfrak{t}^3$, in the first case according as $2//y$ or $4/y$, and in the second case according as $x \equiv -2$ or $x \equiv +2 \bmod 8$.*

The proof of the first sentence has already been given in the proof of theorem VIII. We reconsider cases (*ii*) and (*iii*) of that proof.

(*ii*) $2/y$. Suppose $2^a//y$. Then $\mathfrak{t}^{2a}//(x-t^2\delta)$ since $y^2 = \text{Norm}\,(x-t^2\delta)$ and $\mathfrak{u} \nmid (x-t^2\delta)$ by lemma 2. Hence

$$y^2 = x^3-Dt^6 = \mu^3\alpha^6+3\mu^2\alpha^4t^2\delta+3\mu\alpha^2t^4\delta^2$$

on substituting for x in terms of μ and α and so

$$3\mu = \left(\frac{y}{t^2\alpha\delta}\right)^2 - \frac{3\alpha^2\mu}{t^2\delta} - \frac{\mu^2\alpha^4}{t^2\delta^2}. \tag{17}$$

If $a > 1$ the second and third terms on the right are divisible by $\mathfrak{t}^4$ and the first, by lemma 5, is congruent to 1 mod $\mathfrak{t}^3$. Hence $3\mu \equiv 1$, $\mu \equiv 3 \bmod \mathfrak{t}^3$. If however

[1] $\delta^3 = +11$ in accordance with the convention introduced at the end of part II.

$a = 1$, the third term is still divisible by $\mathfrak{t}^4$ but the second only by $\mathfrak{t}^2$ and so[1] is congruent to 4 mod $\mathfrak{t}^3$. Hence $3\mu \equiv 5$, $\mu \equiv 7$ mod $\mathfrak{t}^3$.

(*iii*) $2/x$ *so* $D \equiv -1$ mod 8. Here α is prime to $\mathfrak{t}$ since y is to 2 and so

$$\mu \equiv \mu\alpha^2 = x - t^2\delta \equiv x - \delta \equiv x + 1 \qquad \text{mod } \mathfrak{t}^3 .$$

Since we have already shown that $2^2 \nmid x$ if μ is not a quadratic residue of 4 this concludes the proof of the lemma.

If μ is not a quadratic residue of 4 we may now write

$$\mu \equiv 3 + 4k \qquad \text{mod } \mathfrak{t}^3 ,$$

where $k = 0$ or 1, and proceed to prove

Theorem IX. *Theorem VIII remains true if* (16) *is replaced by*

$$\mu \equiv D - \delta + 4k + 4l(1+\delta),\ -2D - \delta + 4k + 4l\delta,\ 2 - D - 2\delta + 4k\delta + 4l \quad \text{mod } \mathfrak{u}^3 , \quad (18)$$

where k has just been defined and l may take both values 0 *or* 1.

It is easily verified that only half the numbers which are quadratic residues of $\mathfrak{u}^2$ are quadratic residues of $\mathfrak{u}^3$. Thus if $\beta \equiv 1$ mod $\mathfrak{u}$ then $\beta^2 \equiv 1, 5$ mod $\mathfrak{u}^3$ but $1 + 4\delta$ and $5 + 4\delta$ are not quadratic residues of $\mathfrak{u}^3$. To prove theorem IX we need now only reconsider cases (*ii*) and (*iii*) of theorem VIII and use lemma 8.

(*ii*) $2/y$. Here

$$x \equiv x^3 \equiv y^2 + Dt^6 \equiv 4k + D \qquad \text{mod } 8 ,$$

by lemma 8. Hence

$$\mu = (x - t^2\delta)(1/\alpha)^2 \equiv (D + 4k - \delta)(1/\alpha)^2 \qquad \text{mod } \mathfrak{u}^3$$

and so (18) holds.

(*iii*) $2/x$. This may be similarly dealt with.

17. $2//D$. We consider congruences to powers of $\mathfrak{t}$ where

$$\mathfrak{t} = [2, \delta],\ \mathfrak{t}^2 = [2, \delta^2],\ \mathfrak{t}^3 = [2]$$

Theorem X. *If* $2//D$ *and* (14) *is soluble then either μ is a quadratic residue of* 4 *or*

$$\mu \equiv 1 \pm \delta + \delta^2,\ 1 + D - \delta,\ 1 - D + \delta \qquad \text{mod } \mathfrak{t}^7 = 4[2, \delta] . \qquad (19)$$

If either x or y were even then so would the other be, and then $Dt^6 = x^3 - y^2 \equiv 0$ mod 4 i. e. $2/t$ contrary to $(x, t) = (y, t) = 1$. Hence $2 \nmid xy$. There are two cases (*i*) t even and (*ii*) t odd.

[1] If $\mathfrak{t} \nmid \beta_1$ and $\mathfrak{t} \nmid \beta_2$ then $\beta_1 \equiv \beta_2$ mod $\mathfrak{t}$ since Norm $\mathfrak{t} = 2$; similarly if $\mathfrak{t}^s // \beta_1$ and $\mathfrak{t}^s // \beta_2$ then $\beta_1 \equiv \beta_2$ mod $\mathfrak{t}^{s+1}$.

(*i*) *t even.* Here $x \equiv x^3 \equiv y^2 \equiv 1 \bmod 4$, so $\mu\alpha^2 = x - t^2\delta \equiv 1 \bmod 4$ and μ is a quadratic residue of 4.

(*ii*) *t odd.* Then $x \equiv x^3 \equiv y^2 + Dt^6 \equiv 1 + D \bmod 8$ so

$$\mu\alpha^2 = x - t^2\delta \equiv 1 + D - \delta \qquad \bmod [8] = \mathfrak{t}^9 .$$

But y is odd, so α is prime to $\mathfrak{t}$ and then $(1/\alpha) \equiv 1,\ 1+\delta,\ 1+\delta^2,\ 1+\delta+\delta^2 \bmod [2] = \mathfrak{t}^3$. Hence, by lemma 4,

$$(1/\alpha)^2 \equiv 1,\ 1+2\delta+\delta^2,\ 1+2\delta+2\delta^2,\ 5+3\delta^2 \qquad \bmod \mathfrak{t}^7 , \tag{20}$$

and $\mu = (x - t^2\delta)(1/\alpha)^2$ satisfies (19).

This concludes the proof. We note that the right hand side of (19) remains unaltered when $-D$, $-\delta$ are substituted for $+D$, $+\delta$ respectively.

Let us now consider some numerical examples. If $D \not\equiv \pm 1 \bmod 9$ is cube-free and if h_D is odd the only *a priori* possible value of μ essentially different from $\mu = 1$ is $\mu = \eta$. Thus $\mathfrak{G}$ has at most one generator and $\mathfrak{U}$ at most one generator of infinite order. Since non-trivial solutions (*i. e.* solutions of infinite order) do exist for $D = \pm 2, \pm 18, \pm 22, \pm 30, \pm 38, \pm 50$ the corresponding group $\mathfrak{U}$ has precisely one infinite generator. Theorem X, using table 2, shows that $\mu = \eta$ is impossible for $D = \pm 6, \pm 14, \pm 34, \pm 42$. Hence for these D there are no non-trivial solutions.

Table 2 shows that there are no even values of D with even class-numbers in the range $|D| \leq 50$ under consideration. If, however, any even values of D exist with even class-number they could be treated as when D is odd.

We consider later the cases $D \equiv \pm 1 \bmod 9$.

18. $2^2 // D$. Write

$$D = 4J , \qquad 2 \nmid J .$$

We consider congruences to powers of $\mathfrak{t}$ where

$$\mathfrak{t} = [2, \tfrac{1}{2}\delta^2],\ \mathfrak{t}^2 = [2, \delta],\ \mathfrak{t}^3 = [2] .$$

Theorem XI. *If* $2^2 // D$ *and* (14) *is soluble then either* μ *is a quadratic residue of* 4 *or* (I) *if* $J \equiv -1 \bmod 4$,

$$\mu \equiv 5-\delta,\ 1-2\delta,\ 1+\delta^2,\ 1+\delta-\delta^2 \qquad \bmod \mathfrak{t}^7 , \tag{21}$$

or (II) *if* $T \equiv +1 \bmod 4$,

$$\mu \equiv -1+\tfrac{1}{2}\delta^2,\ 3+\tfrac{3}{2}\delta^2,\ 1+\delta+\tfrac{1}{2}\delta^2,\ 1+\delta+\tfrac{3}{2}\delta^2 \qquad \bmod \mathfrak{t}^7 \tag{22}$$

As $(x, t) = (y, t) = 1$ it is easy to see that one of the three cases holds (*i*) $2 \nmid xy$, $2/t$ (*ii*) $2 \nmid xyt$ (*iii*) $2/x$, $2//y$, $2 \nmid t$.

(*i*) $2 \nmid xy$, $2/t$. This is analogous to case (*i*) in the previous two sections. We have $x \equiv x^3 \equiv y^2 \equiv 1 \bmod 8$ and so $\mu\alpha^2 = x - t^2\delta \equiv 1 \bmod 4$ i. e. μ is a quadratic residue of 4.

(*ii*) $2 \nmid xyt$. Here $x \equiv x^3 = y^2 + Dt^6 \equiv 1 + D \equiv 5 \bmod 8$ and so

$$\mu\alpha^2 = x - t^2\delta \equiv 5 - \delta \qquad \bmod 8 .$$

But α is prime to $\mathfrak{t}$ since y is prime to 2 and so

$$(1/\alpha) \equiv 1,\ 1+\delta,\ 1+\tfrac{1}{2}\delta^2,\ 1+\delta+\tfrac{1}{2}\delta^2 \qquad \bmod \mathfrak{t}^3 = [2] .$$

Hence, by lemma 5,

$$(1/\alpha)^2 \equiv 1,\ 1+2\delta+\delta^2,\ 1+J\delta+\delta^2,\ 5+3J\delta \qquad \bmod \mathfrak{t}^7 . \tag{23}$$

Thus if $J \equiv +1 \bmod 4$, μ is a quadratic residue of $\mathfrak{t}^7$ and *a fortiori* of 4 and if $J \equiv -1 \bmod 4$ one of the congruences (21) holds.

(*iii*) $2/x$, $2//y$, $2 \nmid \mathfrak{t}$. Write $x = 2x'$, $y = 2y'$ so that $2 \nmid y'$ and

$$2x'^3 = y'^2 + Jt^6 \equiv 1 + J \qquad \bmod 8 .$$

Hence $J \not\equiv 3 \bmod 8$ and

$$\left.\begin{aligned} 4/x \text{ if } J \equiv 7 \qquad \bmod 8 . \\ x = 2x' \equiv 1+J \bmod 8 \text{ if } J \equiv 1 \bmod 4 . \end{aligned}\right\} \tag{24}$$

Let $\alpha = \frac{1}{2}\delta^2\alpha'$ so that α' is prime to $\mathfrak{t}$ and

$$\mu\alpha'^2 = (2/\delta^2)^2(x - t^2\delta) \equiv -J + x\delta^2/4 \qquad \bmod \mathfrak{t}^7 . \tag{25}$$

We now consider the two cases $J \equiv 7 \bmod 8$ and $J \equiv 1 \bmod 4$ separately.

(*iii*$_1$) $J \equiv 7 \bmod 8$. Then (24) implies either that the right hand side of (25) is congruent to $1 \bmod \mathfrak{t}^7$ so that μ is a quadratic residue of $\mathfrak{t}^7$ and *a fortiori* of 4 or that it is congruent to $1+\delta^2 \bmod \mathfrak{t}^7$ and then (21) holds.

(*iii*$_2$) $J \equiv 1 \bmod 4$. By (24) the right hand side of (25) is congruent to $-J + (1+J)\delta^2/4 \bmod \mathfrak{t}^7$. Since $(1/\alpha')$ is prime to $\mathfrak{t}$, $(1/\alpha')^2$ satisfies one of the congruences (23) and hence (22) holds.

This concludes the proof of the theorem.

Corollary 1. *If* $2^2//D$ *and* μ *is not a quadratic residue of* 4 *at least one of* (14) *or* (15) *is insoluble.*

For (21) is incompatible with the set of congruences obtained from (22) by writing $-\delta$ for δ.

In particular, precisely as corollary 2 of theorem VIII is derived from corollary 1, we have here also

Corollary 2. *If $2^2//D$, $D \not\equiv \pm 1 \bmod 9$ is cube-free and if h_D is odd, non-trivial solutions do not exist for both $y^2 = x^3 \pm Dt^6$. If non-trivial solutions do exist for one of these equations then the corresponding group $\mathfrak{U}$ has precisely one generator of infinite order.*

We now consider some numerical examples.

Non-trivial solutions actually exist for the values $D = +4, -12, +20$ and -36 which satisfy the conditions of corollary 2. Hence there is precisely one infinite generator for each of the corresponding groups $\mathfrak{U}$. Moreover, by the same corollary, there are no non-trivial solutions for $D = -4, +12, -20, +36$.

We leave for later consideration the cases $D \equiv \pm 1 \bmod 9$.

19. $2^3//D$. As $(x, t) = (y, t) = 1$ it is not difficult to see that one of the three cases holds: (*i*) $2 \nmid xy$, $2/t$ (*ii*) $2 \nmid xyt$ (*iii*) $2//x$, $2^2/y$, $2 \nmid t$. Of these (*iii*) gives rise to the new possibility that $[x - t^2\delta]$ is not the square of an ideal.

Since we are excluding perfect cubes at present, the only values in the range $|D| \leq 50$ under consideration are $D = \pm 24$, ± 40. For all these $D = \pm 2^3 D^*$ where D^* is odd and cube-free and $h_{D^*} = 1$. As before let $\Delta^3 = D^*$. We consider congruences to powers of $\mathfrak{t}$ and $\mathfrak{u}$, the first and second degree prime divisors respectively of 2, where

$$\mathfrak{t} = [2, 1+\Delta],\ \mathfrak{t}^2 = [4, D^*-\Delta],\ \mathfrak{t}^3 = [8, D^*-\Delta]\,,$$

$$\mathfrak{u} = [2, 1+\Delta+\Delta^2],\ \mathfrak{u}^2 = [4, 1+D^*\Delta+\Delta^2],\ \mathfrak{u}^3 = [8, 1+D^*\Delta+\Delta^2]\,.$$

By the discussion in § 12 the only *a priori* possible values of μ are $\mu = 1, \eta$ in cases (*i*) and (*ii*) and $\mu = \lambda, \lambda\eta$ in case (*iii*) where $\lambda > 0$ and $[\lambda] = \mathfrak{u}$. The group $\mathfrak{U}$ has no, has one or has two generators of infinite order according as no, one or all three value of μ essentially distinct from 1 can actually occur in (14). Case (*i*) is completely analogous to case (*i*) previously. It implies that μ is a quadratic residue of 4 i. e. that $\mu = 1$ and so it may be neglected in the rest of this §.

We now treat $D = +24$, $D = -24$, $D = \pm 40$ separately. We shall show that the corresponding group $\mathfrak{U}$ has no, two and one generator of infinite order respectively.

$D = +24$, $\Delta^3 = D^* = 3$. (*ii*) $2 \nmid xyt$. Here $x \equiv x^3 \equiv y^2 \equiv 1 \bmod 8$ and so

$$\begin{aligned} \mu\alpha^2 &= x - 2t^2\Delta \\ &\equiv 1 - 2\Delta \quad \bmod 8 \\ &\equiv 3 \quad \bmod \mathfrak{t}^3\,. \end{aligned}$$

But α is prime to $\mathfrak{t}$, since y is prime to 2, and so $\alpha^2 \equiv 1 \bmod \mathfrak{t}^3$ (lemma 5). Hence

$\mu \equiv 3 \bmod \mathfrak{t}^3$. This is clearly impossible for $\mu = 1$ and it is also false for the only other possibility $\mu = \eta = \Delta^2 - 2 \equiv -1 \bmod \mathfrak{t}^3$.

(*iii*) $2//x$, $2^2/y$, $2\nmid t$. Let $x = 2x'$ where x' is odd and let η_1 denote either 1 or η. The only *a priori* possibility for μ is η, λ where $\lambda > 0$ and $[\lambda] = \mathfrak{u}$, say $\lambda = 2(\Delta - 1)^{-1}$. Then

$$\frac{\eta_1 \alpha^2}{\Delta - 1} = x' - t^2\Delta \equiv x' - \Delta \qquad \text{mod } 4\,.$$

Now α is prime to $\mathfrak{u}$ since $x' - t^2\Delta$ is by lemma 2 and so $(1/\alpha) \equiv 1,\ 1+\Delta,\ \Delta \bmod \mathfrak{u}$ by lemma 4. Hence $(1/\alpha)^2 \equiv 1,\ -\Delta,\ -1+\Delta \bmod \mathfrak{u}^2$ by lemma 5, and then

$$\begin{aligned} \eta_1 &\equiv (x' - \Delta)(\Delta - 1)(1/\alpha)^2 \qquad \text{mod } \mathfrak{u}^2 \\ &\equiv 1 - x' + x'\Delta,\ -1 + (1-x')\Delta,\ x' - \Delta \qquad \text{mod } \mathfrak{u}^2\,. \end{aligned}$$

Since x' is odd this congruence is impossible both for $\eta_1 = 1$ and for $\eta_1 = \eta = \Delta^2 - 2 \equiv 1 + \Delta \bmod \mathfrak{u}^2$.

Hence when $D = +24$ none of the *a priori* possible values of μ essentially different from 1 actually can occur, i. e. $\mathfrak{U}$ has no generators of infinite order.

$D = -24$, $\Delta^3 = D^* = 3$. (*ii*) $2\nmid xyt$. Solutions of this type do exist with $\mu = \eta$. An example is

$$1^3 - 5^2 = -24$$

since $1 + 2\Delta = \mu\alpha^2$ is not a perfect square[1].

(*iii*) $2//x$, $2^2/y$, $2\nmid t$. Solutions do exist of this type i. e. with $\mu = 2\eta_1/(\Delta - 1)$ where $\eta_1 = 1$ or η. An example is

$$(-2)^3 - 4^2 = -24\,.$$

Hence for $D = -24$ solutions exist for at least two, and so for all three *a priori* possible values of μ essentially distinct from 1 i. e. $\mathfrak{U}$ hs two generators of infinite order.

$D = \pm 40$, $\Delta^3 = D^* = 5$. (*ii*) $2\nmid xyt$. Here $x \equiv x^3 \equiv y^2 \equiv 1 \bmod 8$. The only *a priori* possible value of μ essentially different from 1 (which we neglect) is $\mu = \eta$. If this actually occurred we should have

$$\eta\alpha^2 = x \pm 2t^2\Delta \equiv 1 + 2\Delta \qquad \text{mod } 4\,,$$

and so

$$\eta \equiv 1 + 2\Delta,\ 2 - \Delta,\ 1 - \Delta \qquad \text{mod } \mathfrak{u}^2$$

by a familiar argument. This is a contradiction since $\eta = 1 - 4\Delta + 2\Delta^2 \equiv -1 - \Delta$ mod $\mathfrak{u}^2$.

[1] $1 + 2\Delta \equiv -1 \bmod \mathfrak{t}^3$ whereas a perfect square is congruent to $+1$ by lemma 6.

(*iii*) $2//x$, $2^2/y$, $2\nmid t$. Solutions do exist of this type, i. e. with $\mu = \eta_1\lambda$, for both $D = \pm 40$ (see table 1). By the group property of μ and since $\mu = \eta$ was shown not to occur, solutions with $\mu = \lambda$ and $\mu = \eta\lambda$ cannot both occur for the same value of D.

Hence when $D = \pm 40$ precisely one of the *a priori* possible values of μ essentially different from 1 actually occurs i. e. $\mathfrak{U}$ has one generator of infinite order.

20. $2^4//D$. Since $(x, t) = (y, t) = 1$ it is not difficult to see that one of the three cases holds (*i*) $2\nmid xy$, $2/t$ (*ii*) $2\nmid xyt$ (*iii*) $2^2/x$, $2^2//y$, $2\nmid t$.

The only values of D to discuss are $D = \pm 16$, ± 48. Since for these $D \not\equiv \pm 1$ mod 9, G has no factors which are not already factors of $D^* = EF^2$ and $h_{D^*} = 1$, the discussion of § 12 shows that the only *a priori* possible value of μ essentially dissimilar to 1 is $\mu = \eta$. There is thus one or no generator of infinite order according as solutions of infinite order (i. e. non-trivial solutions) do or do not occur.

$D = \pm 48$. Non-trivial solutions occur for both these values of D (table 1). Hence for both $D = \pm$ 48 the group $\mathfrak{U}$ has one infinite generator.

$D = \pm 16$. $\Delta^3 = D^* = 2$. We shall show that no non-trivial solutions exist. It is enough to show that none exist for which $\mu = \eta$. We consider congruences to powers of $\mathfrak{t}$ where

$$\mathfrak{t} = [2, \Delta],\ \mathfrak{t}^2 = [2, \Delta^2],\ \mathfrak{t}^3 = [2]\,.$$

(*i*) $2\nmid xy$, $2/t$. As before, this implies that μ is a quadratic residue of 4, i. e. that $\mu = 1$.

(*ii*) $2\nmid xyt$. Here $x \equiv x^3 \equiv y^2 \equiv 1$ mod 8 and so if $\mu = \eta$ we should have

$$\eta\alpha^2 = x \pm 2\Delta t^2 \equiv 1 \pm 2\Delta \quad \text{mod } 8\,.$$

Hence by a familiar argument

$$\eta \equiv 1+2\Delta,\ 5+\Delta^2,\ 1+2\Delta+3\Delta^2,\ 1+2\Delta^2 \quad \text{mod } \mathfrak{t}^7\,.$$

This is a contradiction since $\eta = -1+\Delta$.

(*iii*) $2^2/x$, $2^2//y$, $2\nmid t$. Write $x = 2^2x'$, $y = 2^2y'$ so y' is odd. Then

$$4x'^3 = y'^2 \pm t^6\,.$$

The upper sign is impossible mod 8 and if the lower is to hold we have $2/x'$. Further, if $\mu = \eta$ we have (taking only the lower sign)

$$\eta\alpha^2 = x + 2t^2\Delta = 4x' + 2t^2\Delta = (\Delta^2)^2(t^2 + x'\Delta^2)\,.$$

If $4/x'$, $t^2 + x'\Delta^2 \equiv 1$ mod 4 and so η would be a quadratic residue of 4, which is untrue. If $2//x'$ we also have a contradiction since then $t^2 + x'\Delta^2 \equiv 1 + 2\Delta^2$ mod $\mathfrak{t}^7 = 4[2, \Delta]$ and so

$$\eta \equiv 1+2\Delta^2,\ 1+2\Delta+3\Delta^2,\ 5+\Delta^2,\ 1+2\Delta \quad \text{mod } \mathfrak{t}^7 ,$$

whereas $\eta = -1+\Delta$.

This concludes the proof that there are no non-trivial solutions when $D = \pm 16$.

21. $2^5//D$. Since $(x, t) = (y, t) = 1$ it is easy to see that either (i) $2\nmid xy$, $2/t$ or (ii) $2\nmid xyt$.

The only values of D to discuss are $D = \pm 32$. Here $\Delta^3 = D^* = 4$, $h_{D^*} = 1$. The only *a priori* possible value of μ other than 1 is $\mu = \eta$ and so $\mathfrak{U}$ has one or no generators of infinite order according as solutions of infinite order (i. e. non-trivial solutions) do or do not exist. We shall show that no non-trivial solutions exist. It is enough to show that none exist with $\mu = \eta$.

We consider congruences to powers of $\mathfrak{t}$ where

$$\mathfrak{t} = [2, \tfrac{1}{2}\Delta^2],\ \mathfrak{t}^2 = [2, \Delta],\ \mathfrak{t}^3 = [2] .$$

(i) $2\nmid xy$, $2/t$. As before this implies that μ is a quadratic residue of 4, i. e. $\mu = 1$.

(ii) $2\nmid xyt$. Here $x \equiv x^3 \equiv y^2 \equiv 1$ mod 8 and so when $\mu = \eta$ we have

$$\begin{aligned} \eta\alpha^2 = x \pm 2t^2\Delta &\equiv 1 \pm 2\Delta \quad \text{mod } 8 \\ &\equiv 1 - 2\Delta \quad \text{mod } \mathfrak{t}^7 . \end{aligned}$$

Hence

$$\eta \equiv 1-2\Delta,\ 1+\Delta^2,\ 5+\Delta,\ 1-\Delta-\Delta^2 \quad \text{mod } \mathfrak{t}^7 ,$$

by a known argument. This contradicts $\eta = 1 + \tfrac{1}{2}\Delta^2$.

22. $D \equiv \pm 1$ *mod* 9, D *cube-free*, h_D *odd.* All the remaining values of D in the range $|D| \leq 50$ which are not perfect cubes fall in this category. We shall consider congruences to powers of $\mathfrak{r}$ and $\mathfrak{s}$ where

$$\mathfrak{r}^2\mathfrak{s} = [3] , \quad \mathfrak{r}\mathfrak{s} = [3, D-\delta] .$$

By the argument of § 12 the only *a priori* possible values of μ are

$$\mu = 1, \eta, \lambda, \lambda\eta ,$$

where λ is defined by

$$\lambda > 0 , \quad [\lambda] = \mathfrak{r}\mathfrak{s}\mathfrak{b}_1^2 .$$

The values λ, $\lambda\eta$ occur if and only if $3/y$. The group $\mathfrak{U}$ has no, or one, or two generators of infinite order according as no, or one, or all three of the values of μ other than 1 actually occur.

Suppose $3/y$ so that $\mu=\eta_1\lambda$ where $\eta_1=1$ or η. Then $3\nmid t$, and so $x\equiv x^3\equiv Dt^6\equiv D$ mod 3. Hence

$$\eta_1\lambda\alpha^2 = x-t^2\delta \equiv D-\delta \not\equiv 0 \quad \bmod \mathfrak{r}^2\mathfrak{s}\,,$$
$$\equiv 0 \quad \bmod \mathfrak{r}\mathfrak{s}\,.$$

Since $\mathfrak{r}+\alpha$ and consequently $\alpha^2\equiv 1$ mod $\mathfrak{r}$, we deduce

$$\eta_1 \equiv (D-\delta)\lambda^{-1} \qquad \bmod \mathfrak{r}\,. \tag{26}$$

We now prove two general theorems according as $\eta\equiv\pm 1$ mod $\mathfrak{r}$.

Theorem XII. *The group* $\mathfrak{U}$ *has at most one infinite generator if* (I) $D\equiv\pm 1$ mod 9, (II) *D is cube-free* (III) *h_D is odd* (IV)$\eta\equiv -1$ mod $\mathfrak{r}$.

For if $\eta\equiv -1$ mod $\mathfrak{r}$ the congruence (26) cannot be true both with $\eta_1=1$ and with $\eta_1=\eta$ i. e. not all three values of μ other than 1 actually occur.

Theorem XIII. *At least one of the two equations $y^2=x^3\pm Dt^6$ has no solutions with $3/y$ if* (I) $D\equiv\pm 1$ mod 9 (II) *D is cube-free* (III) *h_D is odd* (IV) $\eta\equiv +1$ mod $\mathfrak{r}$.

For if (26) is true *either* with $\eta_1=1$ *or* with $\eta_1=\eta$ the corresponding congruence in which the signs of D and δ are simultaneously changed is false *both* for $\eta_1=1$ *and* for $\eta_1=\eta$.

We now consider some numerical examples.

The conditions of theorem XII are satisfied for the following values of D,

$$D=\pm 19,\ \pm 28,\ \pm 35,\ \pm 44\,.$$

Since non-trivial solutions exist for these D (table 1) the corresponding group $\mathfrak{U}$ has precisely one infinite generator.

There are solutions when $D=-17$ both for $\mu=\eta$ and for $\mu=\eta_1\lambda$ since $(-1)^3-4^2=(-2)^3-3^2=-17$. Hence the group $\mathfrak{U}_{-17}$ has two infinite generators. For $D=+17$ there are consequently no solutions either with $\mu=\eta$ (theorem VIII corollary 1) or with $\mu=\eta_1\lambda$ (theorem XIII). Hence there are no non-trivial solutions at all for $D=+17$. Similarly for $D=\pm 37$.

When $D=\pm 10$ there are no solutions with $\mu=\eta$ by theorem X. As a non-trivial solution $(-1)^3-3^2=-10$ does exist for $D=-10$ the corresponding group $\mathfrak{U}_{-10}$ has precisely one infinite generator. By theorem XIII there are consequently no solutions with $3/y$ for $D=+10$ i. e. none with $\mu=\eta_1\lambda$. Since there are also none with $\mu=\eta$ there are none at all.

By a precisely similar argument the group $\mathfrak{U}_{46}$ has no and the group $\mathfrak{U}_{-46}$ precisely one infinite generator. We note further that the solution for $D=-46$,

$$(-7)^3 - 51^2 = -46.2^6$$

must correspond to a μ other than 1 since $3/y$, and hence to the only other occurring value of μ. Consequently this value of μ is also a quadratic residue of 4, i. e. μ is a quadratic residue of 4 for *all* solutions with $D = -46$. This implies that $2/t$ and hence $X = x/t^2$, $Y = y/t^3$ cannot be integers (cf. § 15).

Finally $D = +26$ has a group $\mathfrak{U}$ with two generators. Hence $D = -26$ can have a group $\mathfrak{U}$ with at most one generator by theorem XIII and so precisely one, as non-trivial solutions do exist.

23. $D = G^3$. We discuss now the case when D is a perfect cube. By the remarks at the beginning of part II we may assume

$$G \text{ square-free}, \qquad 3\nmid G .$$

The roots $\delta_1, \delta_2, \delta_3$ of $\delta^3 - D = 0$ are $G, \varrho G, \varrho^2 G$ where ϱ is a complex cube root of unity. Since $\delta_1, \delta_2, \delta_3$ are not all conjugate we must use the "triplets" introduced in § 5 to define the group $\mathfrak{G}$. We recollect that the set of triplets[1] $\{x - t^2\delta_j\}$ form the multiplicative group $\mathfrak{G}$ when squared factors are ignored. We shall first prove

Lemma 9. *The set of triplets $\{x - t^2\delta_j\}$ corresponding to solutions with $3\nmid y$ form a subgroup $\mathfrak{G}^0$ of $\mathfrak{G}$ with one less generator.*

We note that $R(\delta_1) = R(1)$, $R(\delta_2) = R(\delta_3) = R(\varrho)$ and that $(1-\varrho)$ is a prime divisor of 3 in $R(\varrho)$ satisfying

$$(1-\varrho)^2 = -3\varrho .$$

Write $\theta_j = x - t^2\delta_j$ so that

$$\theta_1 = x - Gt^2, \; \theta_2 = \overline{\theta}^3 = x - \varrho G t^2 ,$$

where the bar denotes the complex conjugate. Now it would follow from $3/\theta_2$ that $3/x$, $3/Gt^2$ contrary to $(x, t) = 1$ and $3\nmid G$. Hence $(1-\varrho)^2 \nmid \theta_2$ and it is easy to verify that $(1-\varrho)\nmid\theta_2$ or $(1-\varrho)//\theta_2$ according as $3\nmid y$ or $3/y$. Clearly the set of $\{\theta_j\}$ for which $(1-\varrho)\nmid\theta_2$ form a subgroup $\mathfrak{G}^0$ of $\mathfrak{G}$ which either coincides with $\mathfrak{G}$ or is of index 2, i. e. the set of $\{\theta_j\}$ corresponding to solutions with $3\nmid y$ does this. Further $\mathfrak{G}^0$ cannot coincide with $\mathfrak{G}$ since there is always the trivial solution $(x, y, t) = (G, 0, 1)$ which does not belong to $\mathfrak{G}^0$. Since all the elements of $\mathfrak{G}$ are of order 2 it follows that $\mathfrak{G}^0$ has one fewer generator then $\mathfrak{G}$, which proves the lemma.

[1] cf. § 8.

Suppose now that $3 \nmid y$ so that all the θ_j are prime to 3 (and non-zero). We shall find a bounded set of triplets $\{\mu_j\} = \{\mu_1, \mu_2, \bar{\mu}_2\}$ such that

$$\theta_1 = \mu_1 a^2,\ a \in R(1);\ \theta_2 = \mu_2 \alpha^2,\ \alpha \in R(\varrho)$$

always holds for one of the set, and indeed with μ_1, μ_2, a, α all integers. Since

$$\theta_1 + \varrho\theta_2 + \varrho^2\theta_3 = 0$$

the common factor of any two of the θ_j must also divide the third. This common factor must also divide $\theta_2 - \theta_1 = (1-\varrho)Gt^2$ and $\theta_2 - \varrho\theta_1 = (1-\varrho)x$ and so since $(x, t) = 1$ and the θ_j are prime to $3 = -\varrho^2(1-\varrho)^2$ we have

$$(\theta_1, \theta_2, \theta_3) = (x, G) = K > 0 \qquad \text{(say)}\ .$$

Write $\theta_j = K\varphi_j$ where the φ_j are co-prime in pairs. Now $y^2 = \theta_1\theta_2\theta_3 = K^3\varphi_1\varphi_2\varphi_3$ and K, being a divisor of G, is square-free. Hence $y = K^2 b$, where $b \in R(1)$ is an integer and

$$\varphi_1\varphi_2\bar{\varphi}_2 = \varphi_1\varphi_2\varphi_3 = Kb^2\ .$$

Since $K > 0$ and the φ_j are co-prime in pairs it follows that there are integers $H > 0$, $H \in R(1)$ and $\nu \in R(\varrho)$ such that

$$\varphi_1 = Ha^2, a \in R(1);\ \varphi_2 = \bar{\varphi}_3 = \nu\alpha^2, \alpha \in R(\varrho);\ K = H\nu\bar{\nu} = HN \text{ (say)}\ ,$$

i. e.

$$\theta_1 = KHa^2,\ \theta_2 = \bar{\theta}_3 = K\nu\alpha^2\ .$$

We may therefore put

$$\{\mu_j\} = \{\mu_1, \mu_2, \mu_3\} = \{KH, K\nu, K\bar{\nu}\}\ . \tag{27}$$

Further, by eliminating x between θ_1 and θ_2 we obtain

$$K\nu\alpha^2 - KHa^2 = (1-\varrho)Gt^2$$

i. e.

$$Ha^2 + (1-\varrho)Jt^2 = \nu\alpha^2,\ t \neq 0, a \neq 0\ , \tag{28}$$

where

$$G = JK = HJN\ ,\quad N = \nu\bar{\nu}\ ,\quad H > 0\ . \tag{29}$$

Conversely a solution of (28) gives a solution of the original equation $y^2 = x^3 - G^3t^6$ with $3 \nmid y$. Since the groups $\mathfrak{G}^0$ or $\mathfrak{G}$ involve triplets they are difficult to handle. We now show that we may use a group not involving triplets.

Theorem XIV. *The values of ν/H for which* (28) *is soluble form a multiplicative group $\mathfrak{F}$ if squared factors are ignored with the same number of generators as there are independent generators of infinite order in $\mathfrak{U}$.*

Since the set of triplets $\{\mu_1, \mu_2, \mu_3\}$ of the form which actually occur with solutions of $y^2 = x^3 - G^3t^6$ form the multiplicative group $\mathfrak{G}^0$ when squared factors are ignored the values of $\mu_2/\mu_1 = \nu/H$ *do* form a multiplicative group $\mathfrak{F}$ when squared factors are ignored. Now $(\nu, H) = 1$ since $\nu\bar{\nu}H = NH$ is a divisor of G, which is square free. Thus, since $H > 0$, the ratio ν/H determines ν and H uniquely i. e. by (27) and (29) it determines $\{\mu_j\}$ uniquely. Hence $\mathfrak{F}$ is isomorphic to $\mathfrak{G}^0$ and, in particular, the two groups have the same number of generators, i. e. one fewer than $\mathfrak{G}$ by lemma 9. The theorem now is an immediate consequence of theorem III since $\delta^3 - D = 0$ has just one rational root.

Corollary 1. *If* (28) *is insoluble except, possibly, when* $\nu = H = 1$, *the group* $\mathfrak{U}$ *has no generators of infinite order.*

For then $\mathfrak{F}$ has no generators. In particular, by theorem V,

Corollary 2. *If* $D \neq -1$ *and* (28) *is insoluble except, possibly, when* $\nu = H = 1$ *there are no non-trivial solutions of* $y^2 = x^3 - G^3t^6$.

We now prove a useful lemma.

Lemma 10. *If* $\nu = \pm 1$ *and* (28) *has solutions then* $\nu H = \text{Norm}\ \chi$ *where* $\chi \in R(\sqrt{3})$.

For suppose $\alpha = e + f\varrho$ where e and f are rational integers. By equating coefficients of 1 and ϱ in (28) and eliminating t we obtain

$$\nu H a^2 = e^2 + 2ef - f^2 = (e+f)^2 - 2f^2$$

which proves the lemma.

Since we are assuming $3 \nmid G$ the only values of $D = G^3$ in the range $|D| \leq 50$ are $D = \pm 1$ and $D = \pm 8$. They are both covered by the general theorem due to Nagell [29].

Theorem XV. *If every prime divisor* $p > 0$ *of* G *is of the form* $12n+5$, *the equations* $y^2 = x^3 \pm G^3t^6$ *have no solutions of infinite order (and so no non-trivial solutions except when* $D = -1$).

For Norm $\nu = \nu\bar{\nu} = N \neq 1$ is impossible in $R(\varrho)$ if the factors of N are to be of the required type. Hence $\nu = \pm 1, \pm\varrho, \pm\varrho^2$ and by absorbing factors $\varrho = (\varrho^2)^2$ or ϱ^2 in α^2 we may assume that $\nu = \pm 1$. Hence, by lemma 10, $\nu H = \text{Norm}\ \chi$, $\chi \in R(\sqrt{3})$ and this again implies $\nu H = 1$, i. e. $\nu = H = 1$ (since $H > 0$). Theorem XV now follows from corollary 1 to theorem XIV.

25. *Conclusion.* We have established a number of general theorems and also given the number of generators of infinite order of $\mathfrak{U}$ for all values of D with $|D| \leq 50$. We end with three general remarks.

I. It has not been shown that the solutions listed in table 1 together with the solutions of finite order form a *basis* of the group $\mathfrak{U}$. All that has been shown is that the number of independent generators of infinite order is the same as the number of solutions given in table 1. It is, however, quite straightforward but rather laborious to find a basis from the data given. Indeed the Mordell-Weil proof of theorems I and II depends essentially on the lemma.

Lemma 11. *Suppose $\mathfrak{G}$ has g generators and that we have obtained g solutions $(x^{(l)}, y^{(l)}, t^{(l)})$ of parameter $u^{(l)}$, $(l = 1, \ldots, g)$, one for each generator. Then there is a constant A depending only on the $x^{(l)}, y^{(l)}, t^{(l)}$, and which may be given explicitly, with the following property:*

If (x, y, t) is any solution with parameter u there is a solution (x^*, y^*, t^*) of parameter u^* such that

$$\text{Max}\,(|x^*|, t^{*2}) \leq A \tag{30}$$

and

$$u = u^* + k_1 u^{(1)} + \cdots + k_g u^{(g)},$$

where the k_l are rational integers.

By (30) the set of (x^*, y^*, t^*) is bounded and may be found explicitly by trial-and-error. Clearly the u^* together with the $u^{(l)}$ form a (possibly redundant) basis for $\mathfrak{U}$.

A considerable amount of computation is involved. Numerical examples are given by Billing [2].

II. In all the equations discussed we have found solutions except when we have shown that none exist. There is, however, no certainty that this will continue to happen. In other words our criteria are necessary for solubility but their sufficiency is unproved. It seems to me likely that necessary and sufficient criteria could be obtained by regarding (14) or (28) as congruences to appropriate moduli, but I do not see how this could be proved.

Nevertheless considerable assistance in the search for solutions of $y^2 = x^3 - Dt^6$ may be obtained by regarding (14) or (28) as congruences.

Suppose for example $D = -39$, $\delta^3 = 39$. The only value of $\mu + 1$ which is not excluded in (14) by theorem VIII is $\mu = 4 - \delta$. Then

$$x+t^2\delta = (4-\delta)\alpha^2 \tag{31}$$

and

$$y^2 = x^3+39t^6 .$$

Since $4-\delta \equiv \delta^2 \bmod 4$, $x+t^2\delta$ is a quadratic residue of 4. Hence $2/t$ (cf. proof of theorem VIII). Suppose $t = 2$. Then

$$x \equiv x^3 \equiv y^2 \equiv 1 \mod 24 . \tag{32}$$

It is easiest to examine (31) modulo rational primes which split into three distinct factors in $R(\delta)$. The smallest of these is

$$19 = [19, \delta-1][19, \delta-7][19, \delta-11] = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$$

(say). On regarding (30) with $t = 2$ as a congruence mod $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ in succession we obtain

$$x \equiv N_1-4 \equiv R-28 \equiv N_3-6 \mod 19 ,$$

where N_1 and N_3 are quadratic non-residues or zero and R is a quadratic residue or zero. Hence

$$x \equiv 8, 15 \mod 19 . \tag{33}$$

The least integer satisfying both (32) and (33) is $x = 217$ and indeed

$$(217)^3+39.2^6 = (3197)^2 .$$

III. We have proved incidentally that no *integer* solutions exist for $D = -11$, -39, $+43$, -46, -47 though rational solutions exist. However, my method appears unsuitable for discussing integer as opposed to rational solutions[1]. As a matter of fact, Mordell [23] has shown that in the remaining[2] cases $D = +21$, $+22$, $+29$, $+30$, $+38$, $+50$ where rational but no integral solutions are given in table 1, then integer solutions do not exist.

I am grateful to Professor L. J. Mordell for his criticism and advice.

[1] Integer solutions have been widely discussed. Cf. Mordell [27].

[2] Mordell does not actually consider $D = +50$ in the text, but it can be dealt with by his methods.

Table 1.

Solutions of $y^2 = x^3 - Dt^6$ of infinite order.

D	Solutions						Integers[1]	Refs[2]
	x	y	t	x	y	t		
1		None					—	24
2	3	5	1				+	17
3		None					—	15
4	2	2	1				+	18
5		None					—	15
6		None					—	17
7	2	1	1				+	15
8		None					—	24
9		None					—	15
10		None					—	22
11	3	4	1	15	58	1	+	15
12		None					—	18
13	17	70	1				+	15
14		None					—	17
15	4	7	1				+	15
16		None					—	20
17		None					—	22
18	3	3	1				+	17
19	7	18	1				+	22
20	6	14	1				+	18
21	37	188	3				*M*	15, *M*8
22	71	119	5				*M*	17, *M*8
23	3	2	1				+	15
24		None					—	19
25	5	10	1				+	15
26	3	1	1	35	207	1	+	22
27		None					—	7
28	4	6	1				+	22
29	3,133	175,364	3				*M*	15, *M*14
30	31	89	3				*M*	17, *M*8
31		None					—	15
32		None					—	21
33		None					—	15
34		None					—	17
35	11	36	1				+	22
36		None					—	18
37		None					—	22
38	4,447	291,005	21				*M*	17, *M*14
39	4	5	1	10	31	1	+	15
40	14	52	1				+	19
41		None					—	15
42		None					—	17
43	1,177	40,355	6				—	15
44	5	9	1				+	22
45	21	96	1				+	15
46		None					—	22
47	12	41	1	63	500	1	+	15
48	4	4	1				+	20
49	65	524	1				+	15
50	211	3059	3				*M*	17

[1] (+) non-trivial integer solutions exist; (—) proved not to exist in present paper; (*M*) proved not to exist by Mordell [23]. (A reference to Mordell is given only when necessary).

[2] References are to §§. Those prefixed with an *M* are to Mordell [23].

Table 1 (*contd.*)

Solutions of $y^2 = x^3-Dt^6$ of infinite order.

D	Solutions						Integers	Refs
	x	y	t	x	y	t		
−1		None					+[1]	24
−2	−1	1	1				+	17
−3	1	2	1				+	15
−4		None					−	18
−5	−1	2	1				+	15
−6		None					−	17
−7		None					−	15
−8	2	4	1				+	24
−9	−2	1	1				+	15
−10	−1	3	1				+	22
−11	−7	19	2				−	15
−12	−2	2	1				+	18
−13		None					−	15
−14		None					−	17
−15	1	4	1	109	1,138	1	+	15
−16		None					−	20
−17	−1	4	1	−2	3	1	+	22
−18	7	19	1				+	17
−19	5	12	1				+	22
−20		None					−	18
−21		None					−	15
−22	3	7	1				+	17
−23		None					−	15
−24	−2	4	1	1	5	1	+	19
−25		None					−	15
−26	−1	5	1				+	22
−27		None					−	7
−28	2	6	1				+	22
−29		None					−	15
−30	19	83	1				+	17
−31	−3	2	1				+	15
−32		None					−	21
−33	−2	5	1				+	15
−34		None					−	17
−35	1	6	1				+	22
−36	−3	3	1				+	18
−37	−1	6	1	3	8	1	+	22
−38	11	37	1				+	17
−39	217	3,197	2				−	15
−40	6	16	1				+	19
−41	2	7	1				+	15
−42		None					−	17
−43	−3	4	1	57	2,290	7	+	15
−44	−2	6	1				+	22
−45		None					−	15
−46	−7	51	2				−	22
−47	17	89	2				−	15
−48	1	7	1				+	20
−49		None					−	15
−50	−1	7	1				+	17

[1] The solution (2, 3, 1) of finite order.

Table 2.[1]

Class numbers and units in $R(\sqrt[3]{D})$.

D	h	η [2]	γ [3]
2	1	$-1+\delta$	
3	1	$-2+\delta^2$	
4	1	$-1+\frac{1}{2}\delta^2$	
5	1	$1-4\delta+2\delta^2$	
6	1	$1-6\delta+3\delta^2$	
7	3	$2-\delta$	
9	1	$-2+\delta$	
10	1	$\frac{1}{3}(23+11\delta+5\delta^2)$	
11	2	$1+4\delta-2\delta^2$	$9-4\delta$
12	1	$1+3\delta-\frac{3}{2}\delta^2$	
13	3	$-4-3\delta+2\delta^2$	
14	3	$1+2\delta-\delta^2$	
15	2	$1-30\delta+12\delta^2$	$49+20\delta+8\delta^2$
17	1	$18-7\delta$	
18	1	$1-3\delta+\delta^2$	
19	3	$\frac{1}{3}(2+2\delta-\delta^2)$	
20	3	$1+\delta-\frac{1}{2}\delta^2$	
21	3	$-47+6\delta+4\delta^2$	
22	3	$23+3\delta-4\delta^2$	
23	1	$-41{,}399-3{,}160\delta+6{,}230\delta^2$	
25	1	$1+2\delta-\frac{4}{5}\delta^2$	
26	3	$3-\delta$	
28	3	$\frac{1}{6}(-2-2\delta+\delta^2)$	
29	1	$*-322{,}461{,}439+103{,}819{,}462\delta+370{,}284\delta^2$	
30	3	$1+9\delta-3\delta^2$	
31	3	$-367+54\delta+20\delta^2$	
33	1	$*3{,}742{,}201+97{,}392\delta-394{,}098\delta^2$	
34	3	$613-24\delta-51\delta^2$	
35	3	$\frac{1}{3}(-22+10\delta-\delta^2)$	
36	1	$1+3\delta-\delta^2$	
37	3	$10-3\delta$	
38	3	$-151+55\delta-3\delta^2$	
39	6	$-23+2\delta^2$	$4-\delta$
41	1	$*-211{,}991{,}370{,}839+305{,}478{,}475{,}184\delta$ $-70{,}761{,}183{,}382\delta^2$	
42	3	$1-42\delta+12\delta^2$	
43	12	$-7+2\delta$	$-12+\delta^2$
44	1	$\frac{1}{3}(113-2\delta-\frac{17}{2}\delta^2)$	
45	1	$1{,}081+66\delta-104\delta^2$	
46	1	$*16{,}449{,}049+4{,}590{,}798\delta+1{,}281{,}255\delta^2$	
47	2	$*-592{,}199-69{,}704\delta+64{,}786\delta^2$	$12-\delta$
49	3	$2-\frac{1}{7}\delta^2$	
50	3	$1-\delta+\frac{1}{5}\delta^2$	

[1] [2] [3] See page 271.

[1] Several η and about half the h have been specially computed. Markoff [22] gives a large number of η and a few h. Reid [39] gives the values of h and η for $|D| \leq 10$ as part of a larger table for general cubic fields. Dedekind [8] finds some more values of h using Markoff's table and incidentally proves certain of the η to be fundamental units. Nagell [28] gives a larger table of η and discusses general criteria for a unit η to be the fundamental unit. All these tables except the'last are reproduced by Delaunay and Faddeev [9]. [added in the proof]. There is a table of units for all in Wolfe [45]. I am indebted to Dr. E. S. Selmer for this reference.

[2] These are fundamental units except, possibly, those marked (*), as is proved by Dedekind or by Nagell (loc. cit. supra).

[3] We remember that $\gamma > 0$ and $[\gamma]$ is the square of an ideal but that neither γ nor $\eta\gamma$ is the square of a number of $R(\delta)$. Since the group of ideals is cyclic for $|D| \leq 50$ essentially only one γ occurs.

REFERENCES

[1] Billing, G. "Ueber kubische Diophantische Gleichungen mit endlich vielen Lösungen". Comm. Math. Helv. 9 (1936–37). pp. 161–165.

[2] — "Beiträge zur arithmetischen Theorie ebener kubischer Kurven". Nova Acta Reg. Soc. Scient. Upsaliensis. Ser. IV vol. XI (1938) No. 1, pp. 1–165.

[3] Brunner, O. "Lösungseigenschaften d. kubischen Diophantischen Gleichung $Z^3 - Y^2 = D$". Inaugural dissertation. Zürich 1933.

[4] — "Weitere Untersuchungen über die Kubische Diophantische Gleichung $Z^3 - Y^2 = D$". Comm. Math. Helv. 7 (1934). p. 67.

[5] Chang Kuo-Lung. "On some Diophantine equations $y^2 = x^3 + k$ with no rational solutions". Quarterly J. (Oxford) 19 (1948). pp. 181—188.

[6] Châtelet, F. "Points exceptionnels d'un cubique de Weierstrass". Comptes Rendus (Paris). 210 (1940). p. 90.

[7] — "Groupe exceptionel d'une classe de cubiques". Comptes Rendus (Paris). 210. (1940). p. 200.

[8] Dedekind, R. "Ueber reine kubische Körper". J. f. Math. 121. (1900). 40–123 and Ges. Math. Werke (Braunschweig, 1930). Vol. II, pp. 148–234.

[9] Delaunay, B. N. and Faddeev, D. K. "Theory of irrationals of the third degree" (in Russian). Travaux de l'Institut Stekloff XI (1940).

[10] Euler, L. "Theoremata quorundarum arithmeticorum demonstratio" Theorema 10. Opera Omnia Ser. 1 vol. 2 (= Commentationes Arithmeticae vol. 1) (Lipsiae et Berolini, MCMXV) pp. 38–58 especially pp. 56–58.

[11] Faddeev, D. K. "The equation $x^3 + y^3 = Az^3$". (in Russian). Travaux de l'Institut Stekloff V (1934). pp. 25–40.

[12] Fueter, R. "Ueber kubische Diophantische Gleichungen". Comm. Math. Helv. 2. (1930). pp. 69–89.

[13] Hasse, H. "Bericht über neuere Untersuchungen und Probleme aus d. Theorie d. algebraischen Zahlkörpern", Teil 1: Klassenkörpertheorie". (Berlin, 1930).

[14] — "Klassenkörpertheorie". (Marburg, 1933. Cyclostyled).

[15] Hilbert, D. "Ges. Abhandlungen, Erster Band, Zahlentheorie". (Berlin, 1932).

[16] HOLZER, L. "Ueber die Gleichung $x^3+y^3 = Cz^3$". J. f. Math. 159 (1928). pp. 93–100.

[17] HURWITZ, A. "Ueber ternäre Diophantische Gleichungen dritten Grades". Vierteljahrschrift d. Naturf. Ges. in Zürich. 62. (1917). pp. 207–229.

[18] LIND, C. E. "Ein Analogon zu einem Nagell'schen Satze über kubische Diophantische Gleichungen". Comm. Math. Helv. 9 (1936-7). pp. 156–160.

[19] LUCAS, E. "Sur l'analyse indéterminé du troisième degré". Nouv. Annales de Math. 2, sér. 17 (1878). pp. 507–14.

[20] LUTZ, E. "Sur l'équation $y^2 = x^3-Ax-B$ dans les corps p-adiques". J. f. Math. 177 (1937). pp. 238–247.

[21] — (Same title). Comptes Rendus (Paris) 203 (1936), pp. 20–22. A short resumé of the above but followed by an interesting comment by A. Weil.

[22] MARKOFF, A. "Sur les nombres entiers dépendents d'une racine cubique d'un nombre entier". Mém. de l'Acad. Imp. des Sciences de St. Pétersbourg. VII Série, Tome XXXVIII No. 9 (1882).

[23] MORDELL, L. J. "The Diophantine equation $y^2-k = x^3$". Proc. London Math. Soc. 13 (1914) pp. 60–80. (The closing paragraphs of this paper are misleading since the author was unaware that there is never more than a finite number of integer solutions of the title equation. cf. next paper).

[24] — "Note on the integer solutions of the equation $Ey^2 = Ax^3+Bx^2+Cx+D$". Mess. of Math. 51 (1922). pp. 169–171.

[25] — "On the rational solutions of the indeterminate equation of the third or fourth degree". Proc. Cambridge Phil. Soc. 21 (1922). pp. 179–182.

[26] — "On some Diophantine equations $y^2 = x^3+k$ with no rational solutions". Archiv for Math. og Natur. B. I. L. Nr. 6, 1947.

[27] — "A chapter in the theory of numbers". (Cambridge, 1947).

[28] NAGELL, T. "Ueber die Einheiten in reinen kubischen Zahlkörpern". Skrifter Videnskapselskapet. Christiania, 1922.

[29] — "Ueber die rationalen Punkte auf einigen kubischen Kurven". Tôhoku Math. J. 24 (1924). 48–53.

[30] — "Sur les propriétés arithmétiques des cubiques planes du premier genre". Acta math. 52 (1928–9). pp. 93–126.

[31] — "L'analyse indéterminé du degré supérieur". Mem. des Sci. Math. 39 (1929).

[32] — "Solutions de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre". Skrifter utg. av d. Norske Videnskabs-Akademi. I. Math.-Naturv. Klasse 1935 No. 1.

[33] — "Bemerkungen über d. Diophantische Gleichung $x^3+y^3 = Az^3$". Arkiv f. Math. Astronomik och Fysik 25B No. 5 (1935). pp. 1–6.

[34] — "Ueber die Lösbarkeit gewisser Diophantischer Gleichungen dritten Grades". Comm. Math. Helv. 9 (1936–7). pp. 31–39.

[35] — "Sur la résolubilité des équations Diophantiennes cubiques à deux inconnus dans un domaine relativement algébrique". Nova Act. Reg. Soc. Sci. Upsaliensis, Series IV, Vol. 13 (1940) No. 3.

[36] PÉPIN, FATHER. "Sur la décomposition d'un nombre entier en une somme de deux cubes rationnels". Journal de Math. (Liouville) II^e Sér. t. 15 (1870). pp. 217–236.

[37] — "Sur certains nombres complexes compris dans la formule $a+b\sqrt{-c}$". Journal de Math. (Liouville) III^e Sér. t. 1 (1875). pp. 317–372 especially pp. 360–372.

[38] POINCARÉ, H. "Sur les propriétés arithmétiques des courbes algébriques". Journal de Math. (Liouville) V^e Sér. t.7 (1901). pp. 161–234.

[39] REID, L. W. "Tafel der Klassenzahlen für kubischen Zahlkörpern". Dissertation, Göttingen 1899. Abstract in Amer. J. Math. 23 (1901). pp. 68–84.

[40] SYLVESTER, J. J. "On certain ternary cubic-form equations". Collected Math. Papers (Cambridge 1909) vol. III. pp. 312–391 especially pp. 312–313 and pp. 347–350. Originally appeared Amer. J. Math. vol. II (1878). pp. 280–285, pp. 357–393 and vol. III (1880) pp. 58–88, pp. 179–189.

[41] WEIL, A. "L'arithmétique sur les courbes algébriques". Acta math. 52 (1928–29). pp. 281–315.

[42] — "Sur un théorème de Mordell". Bull. des Sci. Math. 2e Sér. 54 (1930). pp. 182–191.

[43] WEYL, H. "Algebraic theory of numbers". (Princeton, 1940).

[44] WHITTAKER, E. T. and WATSON, G. N. "A course of Modern Analysis". (Cambridge. 4th Edition 1927).

[45] WOLFE, C. "On the indeterminate cubic equation $x^3 + Dy^3 + D^2z^3 - 3Dxyz = 1$." Univ. of California Pub. in Math. 1 No. 16 (1923). pp. 359—369.

The above list is far from being exhaustive. In particular, there are many more papers by NAGELL and others in Scandinavian journals, but references to these will be found in those papers noted here.