There is an immediate application of Theorem 3 to the equation

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

This shows at once that there are only a finite number of integer solutions if $(x, k) = 1$, as happens for example when k is square free. We must solve $f(x, y) = 1$ where $f(x, y)$ is a binary cubic with discriminant $-4k$. Since there are only a finite number of classes of forms with discriminant $-4k$, Thue's theorem in Chapter 22 shows at once that there are only a finite number of integer solutions for x, y.

The result holds for all k as is shown in Chapter 26.

3. We discuss in more detail the integer solutions of the general cubic equation

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 = m. \tag{12}$$

It is known as a particular case of Thue's theorem of Chapter 22 that there are only a finite number of solutions if we suppose that $f(x, y)$ is irreducible. No necessary and sufficient condition for the existence of integer solutions of equation (12) nor a finite algorithm for finding them when they exist are known. However, Baker[3] has recently found an upper bound (a very large one indeed) for the magnitude of the solutions.

Some results are known about the number of solutions and some special equations of the form $ax^3 + dy^3 = m$ can be completely solved. We have seen that it suffices in (12), to consider the case when $m = 1$. Then if one solution is known, we may by means of a linear substitution suppose that $a = 1$.

Let $\theta, \theta', \theta''$ be the roots of the cubic equation

$$t^3 - bt^2 + ct - d = 0, \tag{13}$$

and let $K = Q(\theta)$ be the cubic field over the rational field generated by θ. Two cases arise according as the discriminant $D < 0$ or > 0.

Suppose first $D < 0$. Then combining results of Delaunay[4] and Nagell[5], we have the

Theorem 4

The equation (12) *for* $m = 1$ *has at most three integer solutions except when* $f(x, y) = (a, b, c, d) \sim (1, 0, 1, 1)$ *or* $(1, -1, 1, 1)$, *when there are exactly four solutions, or when* $f(x, y) \sim (1, 0, -1, 1)$, *when there are exactly five solutions.*

The proof requires a detailed investigation and so we shall give only a sketch of the method. We operate in the ring $Z[\theta]$. In this there is one fundamental unit η, and this may be taken to satisfy $0 < \eta < 1$. From equation (13),

$$(x + \theta y)(x + \theta' y)(x + \theta'' y) = 1,$$

and so $x + \theta y$ is a unit in the ring. Hence

$$x + \theta y = \eta^m, \quad m = 0, \pm 1, \pm 2, \ldots \tag{14}$$

and we have to find the integer values of m for which this is possible. The first stage in the proof is to show that equation (14) can be replaced by

$$x + \eta y = \eta^m, \tag{15}$$

and that η is a root of an equation with $d = 1$. The next stage is to show that $m \geqslant 0$ except for the excluded case $\eta^3 + \eta^2 = 1$ when $\eta^{-2} = 1 + \eta$.

We show there is at most one unit for which $xy \neq 0$. Suppose that m_0 is the least positive integer for which a relation

$$x_0 + \eta y_0 = \eta^{m_0} \tag{16}$$

holds, and that x, y, m in equation (15) is a different set.

Put $$m = qm_0 + r, \quad 0 \leqslant r < m_0.$$

It can be shown that $3 \leqslant r \leqslant m_0 - 2$. Put

$$\varepsilon = \eta^r = X + \eta Y + \eta^2 Z. \tag{17}$$

Then $Z \neq 0$ since $r < m_0$. From equations (15), (16)

$$x + \eta y = (x_0 + \eta y_0)^q (X + \eta Y + \eta^2 Z).$$

A congruence mod y_0 shows that $Z \equiv 0 \pmod{y_0}$ and so $|Z| \geqslant y_0$. From equation (17) and the conjugate equations,

$$\pm\sqrt{D}Z = (\eta' - \eta'')\varepsilon + (\eta'' - \eta)\varepsilon' + (\eta - \eta')\varepsilon''.$$

Also $$\eta^3 \geqslant \eta^r = \varepsilon \geqslant \eta^{m_0 - 2},$$

$$|\varepsilon'| = |\varepsilon''| \leqslant |\eta'|^{m_0 - 2} = \left|\frac{x_0 + y_0\eta'}{\eta'^2}\right| < \left|\frac{y_0}{\eta'}\right| + \frac{|y_0| - 1}{|\eta'^2|},$$

since $|x_0| < 1 + |\eta y_0| < 1 + |y_0|$ and $|x_0| = |y_0|$ implies $|y_0| = 1$.

Hence $$\sqrt{|D|}\,|y_0| < 2|\eta'|\varepsilon + 2(1 + |\eta''|)\left(\left|\frac{y_0}{\eta'}\right| + \frac{|y_0| - 1}{|\eta'^2|}\right).$$

Then $$|\eta_1^{q_1}\varepsilon| \leqslant 1 \quad \text{since} \quad |\eta_1^{x_1}\eta^{m_1}\eta^{y_1}| = 1.$$

Hence, since $|\eta'| > 1$,

$$|\sqrt{D}y_0| < 2 + 4(|y_0| + |y_0| - 1) = -2 + 8|y_0|.$$

Then $-D < 64$, and then there can be at most three units.

The cases $D > -64$ arise only for $D = -23, -31, -44$ and these must be investigated in detail.

4. Theorem 4 does not enable us to find the existing integer solutions. All the solutions, however, can be found for some equations of the form

$$ax^3 + by^3 = c.$$

In particular, as was first shown by Delaunay, the equation

$$x^3 + dy^3 = 1,$$

does not present too much difficulty. The integer solutions are trivial when d is a perfect cube. Then if $|d| > 1$, the only solution is $x = 1, y = 0$, and when $|d| = 1$, there is another solution $x = 0, dy = 1$. We may suppose now that $d > 1$ and is free from cubed factors since these can be absorbed in y^3. We consider the cubic field $K = Q(\sqrt[3]{d})$. The integers in K of the form $x + y\sqrt[3]{d} + z\sqrt[3]{d^2}$, where x, y, z are rational integers, form a ring $Z[\sqrt[3]{d}]$, the units in which are those integers η whose norm $N(\eta) = \pm 1$. Let ϵ be the fundamental unit in the ring chosen so that $0 < \epsilon < 1$. Then all the units in $Z[\sqrt[3]{d}]$ are given by

$$\eta = \pm \epsilon^n,$$

where n takes all integer values. The + sign must be taken for the positive units. Then if rational integers x, y satisfy

$$x^3 + dy^3 = 1, \quad \text{i.e. } N(x + y\sqrt[3]{d}) = 1,$$

$\eta = x + y\sqrt[3]{d}$ is a positive unit in the ring. Such a unit will be called a binomial unit.

Theorem 5

The equation $x^3 + dy^3 = 1$ $(d > 1)$ has at most one integer solution with $xy \neq 0$. This is given by the fundamental unit in the ring when it is a binomial unit, i.e. ϵ takes the form $\epsilon = x + y\sqrt[3]{d}$.

We require four lemmas.

Lemma 1

There cannot exist units

$$\eta = P + Q\sqrt[3]{d} + R\sqrt[3]{d^2}, \quad |\eta| > 1, \ QR = 0.$$

Suppose first that $R = 0$. Then $PQ < 0$, and

$$1/|\eta| = P^2 - PQ\sqrt[3]{d} + Q^2\sqrt[3]{d^2} \geqslant 1 + \sqrt[3]{d} + \sqrt[3]{d^2} > 3,$$

a contradiction.
So if $Q = 0$, $PR < 0$, and

$$1/|\eta| = P^2 - PR\sqrt[3]{d} + R^2\sqrt[3]{d^2} > 3.$$

Hence we have to find the positive integers n such that

$$\epsilon^n = x + y\sqrt[3]{d}.$$

Lemma 2

No unit of the types

$$(x + y\sqrt[3]{d})^n, \quad n = \pm 2, \pm 3, \ldots; \qquad (x + y\sqrt[3]{d^2})^n, \quad n = \pm 1, \pm 2, \ldots$$

can be a binomial unit.

We may suppose that the units are positive and so $n > 0$. Take the first type. Expand and equate to zero the terms in $\sqrt[3]{d^2}$, and put $t = dy^3$. This gives three different cases depending on the residue of n (mod 3). Then for $n \equiv 2 \pmod 3$,

$$t^{(n-2)/3} + t^{(n-5)/3}x^3\binom{n}{3} + t^{(n-8)/3}x^6\binom{n}{6} + \cdots + (x^3)^{(n-2)/3}\binom{n}{2} = 0,$$

$n \equiv 1 \pmod 3$,

$$t^{(n-4)/3}\binom{n}{2} + t^{(n-7)/3}x^3\binom{n}{5} + \cdots + (x^3)^{(n-4)/3}\binom{n}{2} = 0,$$

$n \equiv 0 \pmod 3$,

$$t^{(n-3)/3}\binom{n}{1} + t^{(n-6)/3}x^3\binom{n}{4} + \cdots + (x^3)^{(n-3)/3}\binom{n}{2} = 0.$$

Since $t = dy^3$, $(x, t) = 1$. Suppose first that $d > 2$ and so $|x| > 1$. Let p be a prime divisor of x and let p^a be the greatest power of p dividing the binomial coefficient in the highest power of t in the equation above under discussion. We shall show that the remaining terms in the equation are divisible by p^{a+1} thus giving a contradiction.

It will suffice to take the case $n \equiv 1 \pmod 3$. The general term with $r > 0$ is given by

$$t^{(n-3r-1)/3}x^{3r}\frac{n.n-1.\cdots.n-3r-1}{(3r+2)!}.$$

Write this as

$$2\left(\frac{n.n-1}{2!}\right)\left(\frac{n-2.n-3.\cdots.n-3r-1}{1.2.\cdots.3r}\right)\left(\frac{x^{3r}}{(3r+1)(3r+2)}\right)t^{(n-3r-1)/3}.$$

The first two terms in brackets are integers. Now if $p \geqslant 2$, $p^{3r} > 3r + 2$ since $2^{3r} > 3r + 2$, and so the term in the third bracket is divisible by p.

We now take the second type of units, and write $t = d^2y^3$.
Three cases arise:
$n \equiv 2 \pmod 3$,

$$\binom{n}{1}t^{(n-2)/3} + t^{(n-5)/3}x^3\binom{n}{4} + \cdots + (x^3)^{(n-2)/3}\binom{n}{1} = 0,$$

$n \equiv 1 \pmod 3$,

$$t^{(n-1)/3} + t^{(n-4)/3}x^3\binom{n}{3} + \cdots + (x^3)^{(n-1)/3}\binom{n}{1} = 0,$$

$n \equiv 0 \pmod 3$,

$$t^{(n-3)/3}\binom{n}{2} + t^{(n-6)/3}x^3\binom{n}{5} + \cdots + (x^3)^{(n-3)/3}\binom{n}{1} = 0.$$

An argument similar to that for the first type applies.

Suppose finally that $d = 2$. Then it is known that the only rational solutions of $x^3 + 2y^3 = 1$ are $x = 1, y = 0; x = -1, y = 1$ (see Chapter 15), and that $-1 + \sqrt[3]{2}$ is the fundamental unit.

Lemma 3

The square of a unit $\eta \neq \pm 1$ cannot be a binomial unit.

Suppose that

$$\eta = P + Q\sqrt[3]{d} + R\sqrt[3]{d^2}.$$

Then
$$Q^2 + 2PR = 0. \tag{18}$$

Also
$$P^3 + Q^3d + R^3d^2 - 3dPQR = 1, \tag{19}$$

since η is a unit.

We shall show that the only integer solutions of these simultaneous equations are given by $P = 1$, $Q = R = 0$, and $P = Q = 0$, $R = 1$, $d = 1$, and these are obviously excluded.

From equation (19), $(P, R) = 1$, and so equation (18) gives four cases.

(A) $P = q^2$, $R = -2r^2$, $Q = \pm 2qr$,

(B) $P = -q^2$, $R = 2r^2$, $Q = \pm 2qr$,

(C) $P = 2q^2$, $R = -r^2$, $Q = \pm 2qr$,

(D) $P = -2q^2$, $R = r^2$, $Q = \pm 2qr$.

Here q, r are integers. Substituting these in equation (2), we have, on putting $p = dr^3$,

(A′) $-8p^2 \pm 20pq^3 + q^6 = 1$,

(B′) $-8p^2 \pm 20pq^3 + q^6 = -1$,

(C′) $p^2 \pm 20pq^3 - 8q^6 = 1$.

(D′) $p^2 \pm 20pq^3 - 8q^6 = -1$.

Clearly (B′) and (D′) are impossible on taking residues mod 4.
From (A′),

$$(4p \pm 5q^3)^2 = 27q^6 - 2.$$

This is Fermat's equation of which the only solutions are $q = \pm 1, p = 0$. Then $r = 0$, and $P = 1$, $Q = R = 0$.

Next equation (C′) can be written as

$$(p \pm 10q^3)^2 - 108q^6 = 1,$$

or say
$$p_1^2 - 4q_1^3 = 1.$$

Hence $p_1 + 1 = 2q_2^3$, $p_1 - 1 = 2q_3^3$. $q_1 = q_2q_3$.

Then

$$q_2^3 - q_3^3 = 1, \quad q_2 = 1, \quad q_3 = 0 \quad \text{or} \quad q_2 = 0, \quad q_3 = -1.$$

Hence $q = 0$, $p = \pm 1$, $P = 0$, $Q = 0$, $R = d = 1$.

Lemma 4

The cube of a unit $\eta \neq \pm 1$, cannot be a binomial unit.

Let
$$\eta = P + Q\sqrt[3]{d} + R\sqrt[3]{d^2}.$$

Then equating to zero the coefficient of $\sqrt[3]{d^2}$ in η^3, we have

$$P^2R + PQ^2 + R^3Qd = 0. \tag{20}$$

Also
$$P^3 + Q^3d + R^3d^2 - 3PQRd = 1. \tag{21}$$

We shall show that the only solutions of these equations are $P = 1$, $Q = R = 0$ or $P = R = 0$, $Q = 1 = d$, or $P = Q = 0$, $R = 1$, $d = 1$.
Write $(Q, R) = \delta$ and so $(P, d\delta) = 1$.
Then from equation (20)

$$R = \delta^2r, \quad Q = \delta q, \quad (q, r) = 1,$$

and so
$$P^2r + Pq^2 + \delta^3r^2qd = 0,$$

or
$$-r^2q\delta^3d = P(Pr + q^2).$$

But
$$(r, Pr + q^2) = 1. \quad \text{and so } P = pr^2,$$

and
$$-q\delta^3d = p(q^2 + pr^3).$$

Also $(P, d\delta) = 1$ and so $(p, d\delta) = 1$, and $q = ps$.

Then
$$-\delta^3sd = p(ps^2 + r^3).$$

Hence
$$s = tp, \qquad -\delta^3td = t^2p^3 + r^3.$$

Now $t \mid s \mid q$, and since $t \mid r$ and $(q, r) = 1$, then $t = \pm 1$.

Hence
$$\pm\delta^3d = p^3 + r^3. \tag{22}$$

Substituting in equation (21) the values

$$R = r\delta^2, \qquad Q = \pm p^2\delta, \qquad P = pr^2, \qquad PQR = \pm r^3p^3\delta^3,$$

we get
$$p^3r^6 \pm p^6\delta^3d + r^3\delta^6d^2 \pm 3p^3r^3\delta^3d = 1.$$

Replacing δ^3d from equation (22), we have

$$p^3r^6 - p^6(p^3 + r^3) + r^3(p^3 + r^3)^2 + 3p^3r^3(p^3 + r^3) = 1.$$

or
$$-p^9 + r^9 + 6p^3r^6 + 3p^6r^3 = 1. \tag{23}$$

There are several ways of dealing with this equation.

Writing $pr^2 = l$, $r^3 - p^3 = m$, it becomes

$$9l^3 + m^3 = 1.$$

This is our equation with $d = 9$. The fundamental unit is $\varepsilon = -2 + \sqrt[3]{9}$. Also ε^n is a binomial unit only when $n = 1$. This proves the lemma.

Alternatively putting $p^3 = v$, $r^3 = u$, we can verify the identity

$$(u^3 + 6u^2v + 3uv^2 - v^3)U^3 = V^3 + W^3, \tag{24}$$

where

$$U = u^2 + uv + v^2, \qquad V = u^3 + 3u^2v - v^3, \qquad W = 3u^2v + 3uv^2.$$

Hence the only solutions of equations (23) and (24) are given by $UVW = 0$ and so $u = 0$, $v = -1$; $u = 1$, $v = 0$; $u = -1$, $v = 1$.

We can now prove that the nth power of a unit $\eta \neq \pm 1$, is not a binomial unit. We may assume that $0 < \eta < 1$ and $n > 0$. We need prove the statement for $n \equiv 1 \pmod 2$ and $n \not\equiv 0 \pmod 3$.

Write $$X^n = (P + Q\sqrt[3]{d} + R\sqrt[3]{d^2})^n = x + y\sqrt[3]{d}.$$

Then $$X^n + \rho Y^n + \rho^2 Z^n = 0,$$

where $\rho = e^{2\pi i/3}$, and Y, Z are the conjugates of X in K. This equation can be written in various forms depending upon the residue of $n \pmod 3$. Thus when $n \equiv 2 \pmod 3$,

$$X^n + (\rho^2 Y)^n + (\rho Z)^n = 0.$$

Hence $\rho^2 Y + \rho Z$ divides the unit X and so must be a unit, i.e. on substituting for Y, Z, then $-P + 2Q\sqrt[3]{d} - R\sqrt[3]{d^2}$ is a unit.

Hence $$-P^3 + 8Q^3d - R^3d^2 - 6PQRd = \pm 1,$$

also $$P^3 + Q^3d + R^3d^2 - 3PQRd = 1.$$

By addition $$9Qd(Q^2 - PR) = 0, 2,$$

and so either $Q = 0$ or $Q^2 - PR = 0$.

If $Q = 0$, $\eta = P + R\sqrt[3]{d^2}$, and is excluded by Lemma 2.

If $Q^2 - PR = 0$,

$$\frac{1}{\eta} = \frac{1}{P + Q\sqrt[3]{d} + R\sqrt[3]{d^2}}$$

$$= P^2 + Q^2\sqrt[3]{d^2} + R^2\sqrt[3]{d^4} - dQR - PR\sqrt[3]{d^2} - PQ\sqrt[3]{d}$$

$$= P^2 - dQR + (R^2d - PQ)\sqrt[3]{d}$$

is a binomial unit > 1 and is excluded by Lemma 1.

Suppose next that $n \equiv 1 \pmod 3$. Then

$$X^n + (\rho Y)^n + (\rho^2 Z)^n = 0,$$

and so $\rho Y + \rho^2 Z$, i.e. $-P - Q\sqrt[3]{d} + 2R\sqrt[3]{d^2}$ is a unit. Hence

$$P^3 + Q^3d - 8R^3d^2 + 6PQRd = \pm 1.$$

Also $$P^3 + Q^3d + R^3d^2 - 3PQRd = 1.$$

Hence $$9Rd(r^2d - PQ) = 0.$$

Then either $R = 0$ and $P + Q\sqrt[3]{d}$ is a binomial unit and so $n = 1$ is the only possibility from Lemma 2, or $R^2d - PQ = 0$.

Then $$1/\eta = P^2 - dQR + (Q^2 - PR)\sqrt[3]{d^2}$$

is a binomial unit > 1 and this is impossible.

This completes the proof.

Nagell[8] and Ljunggren[9] have generalized the method above and have found more comprehensive results given as

Theorem 6

Let a, b, c be positive integers, $a > b > 1$, $c = 1, 3$, $(ab, c) = 1$, $b = 1$ if $c = 3$. Then the equation

$$ax^3 + by^3 = c \tag{25}$$

has at most one integer solution (x, y), and for this

$$c^{-1}(x\sqrt[3]{a} + y\sqrt[3]{b})^3$$

is either the fundamental unit or its square in the cubic field $Q(\sqrt[3]{d})$ defined by $Q(\sqrt[3]{ab^2})$, excluding however, the equation $2x^3 + y^3 = 3$ which has the two solutions $(1, 1)$ and $(4, -5)$.

Further there is at most one equation (25) with given d which has integer solutions with $xy \neq 0$ except when $d = 2, 20$.

5. Suppose next that $D > 0$ in equation (12). There are now two fundamental units η_1, η_2 and so

$$x + \theta y = \eta_1^l \eta_2^m. \tag{26}$$

It is not often that equations such as (26) are so easily dealt with as in Chapter 27. In general, they prove rather difficult and troublesome as was seen for the equation

$$x^3 - 3xy^2 + y^3 = 1$$

considered in Chapter 23.