CHAPTER 14

Simple Algebraic Considerations

1. Some results require only the definition of an algebraic number, namely, that θ is an algebraic number if it is the root of an equation, reducible or irreducible, over the rational field Q,

$$\theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \cdots + a_n = 0,$$

where the a are rational numbers. Many of these results are classical and are due to Euler and Lagrange.

The equation

$$ax^2 + by^2 = cz^n, \tag{1}$$

where a, b, and c are integers.

Suppose first that n is odd. Consider the classical case when $c = 1$.

Some integer solutions may be found by putting

$$z = ap^2 + bq^2,$$

where p and q are arbitrary integers, and taking

$$x\sqrt{a} + y\sqrt{-b} = (p\sqrt{a} + q\sqrt{-b})^n,$$

$$x\sqrt{a} - y\sqrt{-b} = (p\sqrt{a} - q\sqrt{-b})^n.$$

Then x, y are expressed as polynomials in p and q.

Occasionally as will be seen in Chapter 15 all the integer solutions may be obtained in this way. The proof requires arithmetic theory.

Suppose next that $n = 2m$ is even. Then unless $a = 1$ when a solution is given above for all n, the question becomes more difficult. From Chapter 7, it is seen that now the problem is to find integer solutions for X, Y of the equation

$$z^m = AX^2 + BXY + CY^2$$

for a finite set of integer values of A and B.

These can be reduced to the form (1). Then if $c = c_1^2 + abc_2^2$ or $c = ac_1^2 + bc_2^2$ solutions may be found as before by factorizing c.

The equation

$$w^n = \prod_{\theta} (x + y\theta + z\theta^2), \tag{2}$$

where $\theta = \theta_1, \theta_2, \theta_3$ are roots of the equation

$$t^3 + at^2 + bt + c = 0,$$

where a, b, c are integers.

A partial integer solution is given by

$$x + y\theta_1 + z\theta_1^2 = (p + q\theta_1 + r\theta_1^2)^n,$$
$$x + y\theta_2 + z\theta_2^2 = (p + q\theta_2 + r\theta_2^2)^n,$$
$$x + y\theta_3 + z\theta_3^2 = (p + q\theta_3 + r\theta_3^2)^n,$$
$$w = \prod_{\theta} (p + q\theta + r\theta^2),$$

where p, q, r are arbitrary integers and n runs through the integers.

The general solution depends upon the theory of algebraic numbers and is connected with the units in an algebraic number field.

The equation

$$z^2 = ax^3 + bx^2y + cxy^2 + dy^3, \tag{3}$$

where a, b, c, d are rational numbers.

All the rational solutions are given at once by putting $x = pz$, $y = qz$ where p and q are arbitrary rational numbers. Finding the integer solutions is a different matter. However, as shown by Lagrange, some integer solutions are found without much difficulty when a, b, c, d are integers and $a = 1$. Let $\theta = \theta_1, \theta_2, \theta_3$ be roots of the equation, reducible or irreducible,

$$t^3 + bt^2 + ct + d = 0.$$

Write $$z^2 = (x - \theta_1 y)(x - \theta_2 y)(x - \theta_3 y),$$

and $$x - ty = (p + qt + rt^2)^2, \quad t = \theta_1, \theta_2, \theta_3,$$

where p, q, r are integers. This implies that when we replace t^3 by $-bt^2 - ct - d$ and t^4 by

$$-bt^3 - ct^2 - dt = -b(-bt^2 - ct - d) - ct^2 - dt,$$

the coefficients of t^2 in the above must be zero.

Hence $$q^2 + 2pr - 2qrb + r^2(b^2 - c) = 0.$$

This gives an integer value for p if $r(b^2 - c)$ is even and $2r \mid q^2$. These conditions are easily satisfied, for example, by $r = 2r_1$, $q = 2r_1q_1$. Clearly then x, y and $z = N(p + q\theta + r\theta^2)$ are integers.

The complete integer solution requires arithmetic theory and is given in Chapter 25.

2. The application of both quadratic and cubic irrationalities is sometimes useful. This introduces many parameters satisfying a few equations, and so it is not difficult sometimes to find particular solutions. A simple instance[1] is given by

Theorem 1

The equation

$$y^2 - ax^2 = z^3 + bz + c, \tag{4}$$

where $a \neq 0$, *and* b, c *are rational, has a two parameter rational solution.*

Let $\theta = \theta_1, \theta_2, \theta_3$ be the roots of the equation

$$t^3 + bt + c = 0.$$

Put $$y \pm x\sqrt{a} = \prod_{\theta} (p + q\theta^2 \pm (r + s\theta)\sqrt{a}),$$

where p, q, r, s are rational parameters. Clearly these two equations define x, y as rational numbers and

$$y^2 - ax^2 = \prod_{\theta} ((p + q\theta^2)^2 - a(r + s\theta)^2).$$

Hence equation (4) is satisfied if

$$z - t = (p + qt^2)^2 - a(r + st)^2,$$

for $t = \theta_1, \theta_2, \theta_3$, since

$$z^3 + bz + c = \prod_{t=\theta} (z - t).$$

Multiply out, put $t^4 = -bt^2 - ct$ and equate coefficients of t^0, t, t^2 on both sides. Then

$$z = p^2 - ar^2, \qquad -1 = -cq^2 - 2ars, \qquad 0 = 2pq - bq^2 - as^2.$$

These give

$$p = \frac{bq^2 + as^2}{2q}, \qquad r = \frac{1 - cq^2}{2as},$$

i.e. a two parameter solution.

Another application[2] is to the

Theorem 2

The equation

$$z^3 = ax^2 + by^2 + c \tag{5}$$

has an infinity of integer solutions if a, b, c *are odd integers,* $(a, b) = 1$, *and if when* $a \equiv 0 \pmod 7$, $c \not\equiv b^3 \pmod 7$, *or when* $b \equiv 0 \pmod 7$, $c \not\equiv a^3 \pmod 7$ *and so if* $ab \equiv 0 \pmod 7$, *it suffices if* $c \not\equiv \pm 1 \pmod 7$.

Denote the three roots of $t^3 = c$ by $\theta = \theta_1, \theta_2, \theta_3$. Then, say,

$$ax^2 + by^2 = (z - \theta_1)(z - \theta_2)(z - \theta_3) = f(z),$$

Put

$$z - \theta = a(l + m\theta + n\theta^2)^2 + b(p + q\theta + r\theta^2)^2 = aX^2 + bY^2, \qquad (6)$$

say, where l, m, n, p, q, r are rational integers. Then $f(z)$ can be expressed in the form

$$f(z) = (aX_1^2 + bY_1^2)(aX_2^2 + bY_2^2)(aX_3^2 + bY_3^2),$$

and so we can take

$$x\sqrt{a} + y\sqrt{-b} = \prod_{r=1}^{3} (X_r\sqrt{a} + Y_r\sqrt{-b}).$$

Then
$$x = aX_1X_2X_3 - bX_1Y_2Y_3 - bX_2Y_3Y_1 - bX_3Y_1Y_2,$$
$$y = -bY_1Y_2Y_3 + aX_1X_2Y_3 + aX_2X_3Y_1 + aX_3X_1Y_2,$$

and so x, y are rational integers.

Expanding equation (6) and equating coefficients of θ, θ^2 on both sides, we have the two equations,

$$\begin{aligned} 2mal + 2qbp &= -1 - an^2c - br^2c, \\ 2nal + 2rbp &= -am^2 - bq^2. \end{aligned} \qquad (7)$$

These are linear in l, p and we have four variables in m, n, q, r at our disposal to ensure that l and p are integers. The right-hand sides of equations (7) will be even numbers if

$$m \equiv q \equiv 1 \pmod 2, \qquad n + r \equiv 1 \pmod 2.$$

We impose the condition $mr - qn = \pm 1$. Then l, p will be integers if

$$bq^3 - r - bcr^3 \equiv 0 \pmod a, \qquad -am^3 + n + acn^3 \equiv 0 \pmod b.$$

Solutions are shown to exist for these congruences from the result in Chapter 6 on the solvability of

$$y^2 \equiv x^3 + k \pmod a.$$

No difficulties arise in the proof which now is straightforward.

When $a = b = 1$, a solution is given in terms of an integer parameter t, by

$$x + iy = \prod_{\theta} (1 + t\theta - \tfrac{1}{2}(t^2 + 1)\theta^2 + i(t + \theta)),$$

$$z = 1 - ct(t^2 + 1) + \frac{1}{4}\left(1 + 2t + \frac{c}{4}(t^2 + 1)^2\right),$$

where $i^2 = -1$, $\theta^3 = c$.

A particular case[3] of the equation

$$z^2 = ax^3 + by^3 + c$$

is given by

Theorem 3

The equation

$$z^2 - (27abd)^2 = ab^2x^3 + y^3, \quad ab \neq 0, \tag{8}$$

where a, b, d are integers, has an infinity of integer solutions.

Consider the equation

$$z^2 - k^2 = ab(x^3 + cy^3), \quad abc \neq 0, \tag{9}$$

Denote by $\theta = \theta_1, \theta_2, \theta_3$ the roots of $t^3 = c$. Take

$$z + k = a \prod_{\theta} (p + q\theta + r\theta^2), \tag{10}$$

$$z - k = b \prod_{\theta} (p_1 + q_1\theta + r_1\theta^2), \tag{11}$$

where the p, p_1, etc. are integers.
Then

$$z^2 - k^2 = ab \prod_{\theta} (P + Q\theta + R\theta^2) = ab(P^3 + cQ^3 + c^2R^3 - 3cPQR),$$

and we take

$$\begin{aligned} P &= pp_1 + c(qr_1 + q_1r) = x, \\ Q &= pq_1 + p_1q + crr_1 = y, \\ R &= pr_1 + p_1r + qq_1 = 0. \end{aligned} \tag{12}$$

From equations (10) and (11),

$$2k = a(p^3 + cq^3 + c^2r^3 - 3cpqr) - b(p_1^3 + cq_1^3 + c^2r_1^3 - 3cp_1q_1r_1). \tag{13}$$

The six variables p, q, r, p_1, q_1, r_1 satisfy the two equations (12) and (13) and particular solutions may be found without difficulty.

Take $p_1 = q, q_1 = -r, r_1 = 0$. Then equation (13) is satisfied.

Also $$x = pq - cr^2, \quad y = -pr + q^2, \quad z - k = b(q^3 - cr^3), \tag{14}$$

$$2k = a(p^3 + cq^3 + c^2r^3 - 3cpqr) - b(q^3 - cr^3). \tag{15}$$

Take now $c = b/a$. Then equation (15) becomes

$$2k = ap^3 + 2b^2r^3/a - 3bpqr, \tag{16}$$

and equation (9) becomes

$$z^2 - k^2 = abx^3 + b^2y^3. \tag{17}$$

DIOPHANTINE EQUATIONS

L. J. MORDELL

ST. JOHN'S COLLEGE
CAMBRIDGE, ENGLAND

1969

ACADEMIC PRESS London and New York

ACADEMIC PRESS INC. (LONDON) LTD.
Berkeley Square House, Berkeley Square, London, W1X 6BA

U.S. Edition published by
ACADEMIC PRESS INC.
111 Fifth Avenue, New York, New York 10003

LIBRARY OF CONGRESS CATALOG CARD NUMBER: 68–9112

PRINTED IN GREAT BRITAIN BY WILLIAM CLOWES AND SONS LTD
LONDON AND BECCLES