REFERENCES

1. H. Hasse. Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen. *J. reine angew. Math.*, **152** (1923), 129–148; also 205–224.
2. L. Holzer. Minimal solutions of diophantine equations. *Can. J. Math.*, **11** (1950), 238–244.
3. L. J. Mordell. On the equation $ax^2 + by^2 - cz^2 = 0$. *Monatshefte für Math.*, **55** (1951), 323–327.
4. T. Skolem. On the diophantine equation $ax^2 + by^2 + cz^2 = 0$. *Rendiconti di Matematica e delle sue applicazioni* (5), **11** (1952), 88–102.
5. L. J. Mordell. On the magnitude of the integer solutions of the equation $ax^2 + by^2 + cz^2 = 0$. *J. number theory*, **I** (1968), 1–3.
6. M. Kneser. Kleine Lösungen der diophantischen Gleichung $ax^2 + by^2 = cz^2$. *Abh. Math. Sem. Hamburg*, **23** (1959), 163–173.
7. J. W. S. Cassels. Bounds for the least solution of homogeneous quadratic equations. *Proc. Camb. Phil. Soc.*, **51** (1955), 262–264. Addendum, *ibid.* **52** (1956), 664.
8. H. Davenport. Note on a theorem of Cassels. *Proc. Camb. Phil. Soc.*, **53** (1957), 539–540. Addendum, *ibid.* **52** (1956), 664.
9. B. J. Birch and H. Davenport. Quadratic equations in several variables. *Proc. Camb. Phil. Soc.*, **54** (1958), 135–138.
10. Z. I. Borevich and I. R. Shafarevich. "Number-theory", Chapter I. Academic Press, New York and London (1966).
11. L. J. Mordell. Integer solutions of simultaneous quadratic equations. *Abh. Math. Sem. Hamburg*, **23** (1959), 124–143.
12. H. P. F. Swinnerton-Dyer. Rational zeros of two quadratic forms. *Acta Arith.*, **9** (1964), 260–270.

CHAPTER 8

Pell's Equation

1. Theorem 1

Let D be a positive integer which is not a perfect square. Then the equation

$$y^2 - Dx^2 = 1 \tag{1}$$

has an infinity of integer solutions. If $(x, y) = (U, T)$ where $T > 0$, $U > 0$ is the solution with least positive x, all the solutions are given by

$$y + x\sqrt{D} = \pm(T + U\sqrt{D})^n, \tag{2}$$

where n is an arbitrary integer.

We ignore the trivial solution $y = \pm 1$, $x = 0$ given by $n = 0$.

The proof of (1) follows easily from a result on Diophantine approximation given by

Lemma 1

Let θ be an irrational number and $q > 1$ an arbitrary positive integer. Then there exist integers x and y such that if $L = y - x\theta$,

$$|L| < 1/q, \qquad 0 < x \leqslant q. \tag{3}$$

Let x take the values $0, 1, 2, \ldots, q$ and let y be such an integer that $0 \leqslant L < 1$. Then $q + 1$ values for L arise lying in the q semi-open intervals

$$\left[\frac{r}{q}, \frac{r+1}{q}\right), \quad r = 0, 1, \ldots, q - 1.$$

Hence two of the values of L corresponding to say (x_1, y_1) and (x_2, y_2), where $x_1 \neq x_2$, say $x_1 > x_2$, lie in the same interval and so

$$|y_1 - y_2 - (x_1 - x_2)\theta| < 1/q.$$

Then (3) follows on putting $y = y_1 - y_2$, $x = x_1 - x_2$. On replacing (3) by

$$|y - x\theta| < 1/x,$$

it follows that there are an infinity of integer solutions of this inequality.

Lemma 2

A number $m = m(D)$, e.g. $m = 1 + 2\sqrt{D}$, exists such that

$$|y^2 - Dx^2| < m,$$

for an infinity of integers, x, y.

Take $\theta = \sqrt{D}$ in (3) and so integers (x, y) exist such that

$$|y - x\sqrt{D}| < 1/|x|.$$

Then

$$|y + x\sqrt{D}| = |y - x\sqrt{D} + 2x\sqrt{D}| < 2|x|\sqrt{D} + 1/|x|,$$

and so

$$|y^2 - Dx^2| < 2\sqrt{D} + 1/x^2 < 2\sqrt{D} + 1.$$

We now deduce the existence of an integer solution of equation (1). There exists an integer k such that $|k| < m$ and

$$y^2 - Dx^2 = k$$

has an infinity of integer solutions. We may suppose there are two, say (x_1, y_1) and (x_2, y_2), such that

$$x_2 \equiv x_1, \qquad y_2 \equiv y_1 \pmod{k}, \qquad (x_2, y_2) \neq (-x_1, -y_1).$$

From

$$y_1^2 - Dx_1^2 = k, \qquad y_2^2 - Dx_2^2 = k,$$

we have by multiplication,

$$(y_1y_2 - Dx_1x_2)^2 - D(y_1x_2 - y_2x_1)^2 = k^2.$$

Write

$$y_1y_2 - Dx_1x_2 = kY, \qquad y_1x_2 - y_2x_1 = kX.$$

Clearly X, Y are integers, $X \neq 0$ and

$$Y^2 - DX^2 = 1.$$

We now deduce an infinity of solutions. Let $(x, y) = (U, T)$ where $U > 0$, $T > 0$, and U is the least value of X. Then an infinity of solutions (x_n, y_n) with $x_n > 0, y_n > 0$ are given by taking

$$y_n + x_n\sqrt{D} = (T + U\sqrt{D})^n, \qquad y_n - x_n\sqrt{D} = (T - U\sqrt{D})^n,$$

where n is any positive integer.

All such solutions are given by these formulae.
For suppose (x, y) is a solution not so given. Then for some positive integer n,

$$(T + U\sqrt{D})^n < y + x\sqrt{D} < (T + U\sqrt{D})^{n+1}.$$

Then

$$1 < (y + x\sqrt{D})(y_n - x_n\sqrt{D}) < T + U\sqrt{D}.$$

Write

$$(y + x\sqrt{D})(y_n - x_n\sqrt{D}) = Y + X\sqrt{D}.$$

and so

$$Y + X\sqrt{D} < T + U\sqrt{D}, \qquad Y^2 - DX^2 = 1.$$

Since $Y + X\sqrt{D} > 1$, and $0 < Y - X\sqrt{D} < 1$, then $X > 0$, $Y > 0$. This contradicts the definition of T, U.

The solutions with

$$x < 0, y < 0 \quad \text{are given by} \quad y + x\sqrt{D} = -(T + U\sqrt{D})^n,$$

$$x < 0, y > 0 \quad \text{are given by} \quad y + x\sqrt{D} = (T + U\sqrt{D})^{-n},$$

$$x > 0, y < 0 \quad \text{are given by} \quad y + x\sqrt{D} = -(T + U\sqrt{D})^{-n},$$

where n is a positive integer.

Corollary

If d is a given integer, there exists an infinity of solutions with $x \equiv 0 \pmod{d}$.

This is obvious from $Y^2 - Dd^2X^2 = 1$.

In the study of the units of quadratic fields, say $Q(\sqrt{d})$, a Pellian equation takes the form

$$y^2 - dx^2 = 4.$$

If now $(x, y) = (u, t)$, $u > 0$, $t > 0$ is the solution with least x, then it can be shown similarly that the general solution is given by

$$\frac{y + x\sqrt{d}}{2} = \pm\left(\frac{t + u\sqrt{d}}{2}\right)^n,$$

where n takes all integer values.

The solution of the equation

$$y^2 - Dx^2 = -1 \tag{4}$$

is a much more difficult question and simple explicit conditions for solvability are not known. A necessary condition is that D is not divisible by 4 or by any prime $\equiv 3 \pmod 4$. It is easily proved that the equation is solvable when $D = p$ is a prime $\equiv 1 \pmod 4$.

For let $(x, y) = (U, T)$ be the fundamental solution of $y^2 - px^2 = 1$. Then $U \equiv 0$, $T \equiv 1 \pmod 2$. Write

$$\frac{T+1}{2} \cdot \frac{T-1}{2} = p\left(\frac{U}{2}\right)^2.$$

Then either

$$\frac{T+1}{2} = pa^2, \qquad \frac{T-1}{2} = b^2,$$

or

$$\frac{T+1}{2} = a^2, \qquad \frac{T-1}{2} = pb^2,$$

where a, b are integers. The second set gives $a^2 - pb^2 = 1$, and contradicts the definition of the fundamental solution.