

# 7

## The Cubic Analogue of Pell's Equation

In looking for a higher-degree version of Pell's equation, a natural choice is the equation

$$x^3 - dy^3 = k,$$

where  $d$  is a noncubic integer. However, it turns out that the solutions of such equations are not very numerous, nor do they exhibit the nice structure found in the quadratic case. This chapter will begin with an investigation of this type before treating a better analogue that admits a theory comparable to the quadratic version. This is the equation:

$$x^3 + cy^3 + c^2z^3 - 3cxyz = k,$$

where  $c$  is any integer other than a perfect cube and  $k$  is an integer. In this chapter we will see how this equation comes about and examine its theory. It will turn out, as in the quadratic case, that there is a fundamental solution; however, this solution is not so neatly obtained and some ad hoc methods are needed.

Sections 6.2 and 6.3 can be skipped, since they are independent of the rest of the chapter.

### 6.1 The Equation $x^3 - dy^3 = 1$ : Initial Skirmishes

**Exercise 1.1.** Suppose  $d = r^3$ , a cubic integer. By using the factorization  $x^3 - r^3y^3 = (x - ry)(x^2 + rxy + r^2y^2)$ , prove that any solution  $(x, y)$  in integers of  $x^3 - dy^3 = \pm 1$  must satisfy  $x^2 + rxy + r^2y^2 = 1$ . Use this fact to deduce that either  $x$  or  $y$  must vanish and so obtain all possible solutions of  $x^3 - r^3y^3 = \pm 1$ .

**Exercise 1.2.**

- (a) Verify that  $x^3 - dy^3 = 1$  has a solution with  $x$  and  $y$  both nonzero when  $d$  has the form  $s^3 - 1$  for some integer  $s$ .
- (b) Try to determine solutions of  $x^3 - 7y^3 = 1$  other than  $(x, y) = (1, 0), (2, 1)$ .

**Exercise 1.3.**

- (a) Prove that  $x^3 - dy^3 = 1$  has a solution for which  $y = 2$  if and only if  $d = u(64u^2 + 24u + 3)$  for some integer  $u$ .
- (b) Determine a solution in nonzero integers of  $x^3 - 43y^3 = 1$ .

**Exercise 1.4.**

- (a) Prove that  $x^3 - dy^3 = 1$  has a solution for which  $y = 3$  if and only if  $d = u(27u^2 + 9u + 1)$ .
- (b) Determine a solution in nonzero integers for  $x^3 - 19y^3 = 1$  and for  $x^3 - 37y^3 = 1$ .

**Exercise 1.5.** Suppose that  $x$  and  $y$  are nonzero integers for which  $x^3 - dy^3 = 1$ . This equation can be rewritten as  $dy^3 = (x - 1)(x^2 + x + 1)$ .

- (a) Verify that the greatest common divisor of  $x - 1$  and  $x^2 + x + 1$  is equal to 3 when  $x \equiv 1 \pmod{3}$  and to 1 otherwise.
- (b) Prove that  $x^2 + x + 1$  is never divisible by 9.
- (c) Deduce from (a) and (b) that  $x^2 + x + 1$  must be of the form  $rv^3$  or  $3rv^3$ , where  $r$  is an odd divisor of  $d$ .

**Exercise 1.6.** Suppose in Exercise 1.5 that  $x^2 + x + 1 = v^3$ .

- (a) Give a numerical example to show that this equation actually has a solution for which  $x$  and  $v$  are both nonzero.
- (b) Find nonzero integers  $x$  and  $y$  for which  $x^3 - 17y^3 = 1$ .

**Exercise 1.7.** Suppose in Exercise 1.5 that  $x^2 + x + 1 = 3v^3$ , so that  $x \equiv 1 \pmod{3}$ . Setting  $x = 3u + 1$ , obtain the equation  $(u + 1)^3 = u^3 + v^3$  and obtain from Fermat's last theorem that this case is not possible. (See **Exploration 7.1**.)

**Exercise 1.8.** Make a table of some integers  $d$  with  $2 \leq d \leq 100$  for which  $x^3 - dy^3 = 1$  has at least one solution with  $xy \neq 0$ . List the solutions. Did you find any values of  $d$  for which there are two such solutions?

## 7.2 The Algebraic Integers in $\mathbf{Q}(\sqrt{-3})$

We have seen that  $x^3 - dy^3 = 1$  is nontrivially solvable for certain values of  $d$ . Rewriting this equation as  $x^3 + (-1)^3 = dy^3$ , we see that we have to study equations of the form  $x^3 + z^3 = dy^3$ . One way to approach this is to factor the left side as  $(x + z)(x + \omega z)(x + \omega^2 z)$ , where  $\omega = \frac{1}{2}(-1 + \sqrt{-3})$  is an imaginary cube root of unity; thus,  $\omega^3 = 1$  and  $\omega^2 + \omega + 1 = 0$ . This can be treated as a factorization in the quadratic field  $\mathbf{Q}(\sqrt{-3}) \equiv \{p + q\sqrt{-3} : p, q \in \mathbf{Q}\}$  treated in Section 4.3. The set  $\mathbf{Q}(\sqrt{-3})$  is closed under addition, subtraction, multiplication, and division by nonzero elements. The norm  $N(a + b\sqrt{-3})$  of numbers of the

form  $a + b\sqrt{-3}$  is defined by the product of the number and its surd conjugate  $a - b\sqrt{-3}$ , namely  $a^2 + 3b^2$ . Note that the norm is always nonnegative.

Recall that a number  $\theta$  is an algebraic integer in  $\mathbf{Q}(\sqrt{-3})$  if and only if it is a root of a quadratic equation of the form  $t^2 + bt + c = 0$ , where  $b$  and  $c$  are integers. Normally, the reciprocal of an algebraic integer is not an algebraic integer. An algebraic integer  $\theta$  is a *unit* if  $\theta$  and its reciprocal  $1/\theta$  are both algebraic integers. The set of algebraic integers in  $\mathbf{Q}(\sqrt{-3})$  will be denoted by  $I$ . This set contains the ordinary integers.

**Exercise 2.1.**

- (a) Explain why  $\omega^2 + \omega + 1 = 0$ .
- (b) Verify that  $\sqrt{-3} = \omega - \omega^2 = 1 + 2\omega$ .
- (c) Prove that  $\mathbf{Q}(\sqrt{-3})$  is the set of numbers of the form  $r + s\omega$ , where  $r$  and  $s$  are rational.
- (d) Prove that the surd conjugate of  $\omega$  is  $\omega^2$ , and thus the surd conjugate of  $r + s\omega$  is  $r + s\omega^2$ .

**Exercise 2.2.** Let  $\alpha$  and  $\beta$  be members of  $\mathbf{Q}(\sqrt{-3})$ . Prove that  $N(\alpha\beta) = N(\alpha)N(\beta)$ .

**Exercise 2.3.** Let  $\theta = r + s\omega$ . Verify that its reciprocal  $1/\theta$  is equal to  $(r + s\omega^2)/(r^2 - rs + s^2)$ .

**Exercise 2.4.**

- (a) Suppose that  $\theta$  belongs to  $I$ . Prove that  $N(\theta)$  is an ordinary nonnegative integer and vanishes only when  $\theta = 0$ .
- (b) Prove that  $\theta$  is a unit if and only if  $N(\theta) = 1$ .
- (c) Suppose that  $r + s\omega$  is a unit, so that  $r^2 - rs + s^2 = 1$ . Prove that  $2r - s$  is an ordinary integer. Deduce that  $r$  and  $s$  are integers for which  $(2r - s)^2 + 3s^2 = 4$ , so that  $(r, s) = (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)$ .
- (d) Prove that the only units in  $I$  are  $\pm 1, \pm\omega$  and  $\pm\omega^2$ . ♠

Analyzing the equation  $x^3 + z^3 = dy^3$  involves examining the factorization of  $x^3 + z^3$ . In the following exercises we will develop a theory of factorization for the system  $I$  that is similar to that for ordinary integers. This will involve notions of divisibility and primality as well as a version of the fundamental theorem of arithmetic that allows each algebraic integer to be decomposed as a product of primes. The development will involve an adaptation of the Euclidean algorithm.

Let  $\alpha$  and  $\beta$  be members of  $I$ . We say that  $\beta|\alpha$  (" $\beta$  divides  $\alpha$ ") if  $\alpha = \beta\gamma$  for some  $\gamma$  in  $I$ . Every member of  $I$  divides 0 and is divisible by each of the units. We say that  $\rho$  in  $I$  is prime if  $N(\rho) \neq 1$  and it is divisible only by numbers of the form  $\epsilon$  and  $\epsilon\rho$ , where  $\epsilon$  is a unit. We will see that an ordinary prime integer may or may not be a prime in  $I$ .

**Exercise 2.5.**

- (a) Suppose that  $\rho$  belongs to  $I$  and that  $N(\rho)$  is an ordinary prime integer. Prove that  $\rho$  must be prime.
- (b) Deduce from (a) that  $1 - \omega$  is a prime.

**Exercise 2.6.** We show that although  $N(2)$  is composite, 2 is actually prime in  $I$ . This demonstrates that the converse of Exercise 2.5(a) is not true.

- (a) Prove that  $N(2) = 4$ .
- (b) Suppose that  $2 = (p + q\omega)(r + s\omega)$  is a product of two members of  $I$ , neither of which is a unit. Prove that  $p^2 - pq + q^2 = \pm 2$ , so that  $(2p - q)^2 + 3q^2 = \pm 8$ . Show that this equation has no solutions in integers  $p$  and  $q$  and deduce from the contradiction that 2 must be prime in  $I$ .

**Exercise 2.7.** Verify that  $3 = -[\omega(1 - \omega)]^2$ , so that 3 is not prime in  $I$  (although it is an ordinary prime).

**Exercise 2.8.** Let  $\alpha$  and  $\beta$  be two members of  $I$ . We can write  $\alpha/\beta$  in the form  $u + v\omega$ , where  $u$  and  $v$  are rational (check that this can be done!). Suppose that  $m$  and  $n$  are integers for which  $|u - m| \leq \frac{1}{2}$  and  $|v - n| \leq \frac{1}{2}$ .

- (a) Verify that  $N((u - m) + (v - n)\omega) \leq \frac{3}{4}$ .
- (b) Let  $\gamma = m + n\omega$  and  $\delta = \alpha - \beta\gamma$ . Verify that  $\alpha = \gamma\beta + \delta$  and that  $N(\delta) \leq \frac{3}{4}N(\beta) < N(\beta)$ . ♠

The result of Exercise 2.7(b) is the analogue of the ordinary division algorithm in which we divide a number  $\beta$  into  $\alpha$  and get a quotient  $\gamma$  and a remainder  $\delta$  “smaller” than the divisor. In this case, the measure of size of a number is not the absolute value but the norm. We can now set up the Euclidean algorithm in the same way as for ordinary integers. Suppose that we are given two algebraic integers  $\alpha$  and  $\beta$ . By repeating division, we can obtain

$$\alpha = \gamma\beta + \beta_1,$$

$$\beta = \gamma_1\beta_1 + \beta_2,$$

$$\beta_1 = \gamma_2\beta_2 + \beta_3,$$

and so on, where  $N(\beta) > N(\beta_1) > N(\beta_2) > N(\beta_3) > \cdots \geq 0$ . Since the norms constitute a decreasing sequence of nonnegative integers, the process cannot go on forever, and we will eventually arrive at an exact division:

$$\beta_{k-2} = \gamma_{k-1}\beta_{k-1} + \beta_k,$$

$$\beta_{k-1} = \gamma_k\beta_k,$$

where  $\beta_k$  is nonzero.

**Exercise 2.9.**

- (a) Prove that  $\beta_k$  must be a common divisor of  $\alpha$  and  $\beta$ .
- (b) Suppose  $\delta$  is a divisor of  $\alpha$  and  $\beta$ . Prove that  $\delta$  is a divisor of  $\beta_k$ . ♠

Let  $\alpha$  and  $\beta$  belong to  $I$ . A *greatest common divisor* of  $\alpha$  and  $\beta$  is an element of  $I$  that divides both  $\alpha$  and  $\beta$ , and in turn is divisible by every common divisor of  $\alpha$  and  $\beta$ . The number  $\beta_k$  produced by the Euclidean algorithm in Exercise 2.8 is a greatest common divisor of  $\alpha$  and  $\beta$ . We say that  $\alpha$  and  $\beta$  are *coprime* if the only common divisors of  $\alpha$  and  $\beta$  are units.

**Exercise 2.10.** Let  $\alpha, \beta$  belong to  $I$ . Suppose  $\rho$  and  $\sigma$  are two greatest common divisors of  $\alpha$  and  $\beta$ . Prove that  $\rho = \sigma\epsilon$  for some unit  $\epsilon$ .

**Exercise 2.11.**

- (a) Suppose that the Euclidean algorithm of Exercise 2.8 is carried out. Observe that

$$\beta_{i+1} = \beta_{i-1} - \gamma_i \beta_i$$

for  $1 \leq i \leq k-1$  (where  $\beta_0 = \beta$ ). Use these facts to show that  $\beta_k$  can be written in the form  $\xi\alpha + \eta\beta$ , where  $\xi$  and  $\eta$  belong to  $I$ .

- (b) Prove that every greatest common divisor of  $\alpha$  and  $\beta$  can be written in this form.

**Exercise 2.12.** Let  $\alpha$  and  $\beta$  be a coprime pair in  $I$ .

- (a) Prove that there are numbers  $\xi, \eta \in I$  for which

$$1 = \xi\alpha + \eta\beta.$$

- (b) Let  $\mu \in I$  and  $\beta|\alpha\mu$ . Prove that  $\beta|\mu$ . ♠

With these results in hand, we are in a position to prove the fundamental theorem of arithmetic for  $I$ , that, up to units, each member of  $I$  can be uniquely written as a product of primes in  $I$ .

**Exercise 2.13.**

- (a) Let  $\alpha$  be a nonprime member of  $I$ . Prove that  $\alpha$  can be written as a product  $\beta\gamma$  where the norms  $N(\beta)$  and  $N(\gamma)$  are strictly less than  $N(\alpha)$ . Extend this result to show that  $\alpha$  can be written as a product  $\rho_1\rho_2 \cdots \rho_k$  of primes.
- (b) Suppose that  $\alpha = \rho_1\rho_2 \cdots \rho_k = \sigma_1\sigma_2 \cdots \sigma_l$  are two representations of  $\alpha$  as a product of primes in  $I$ . Use Exercise 2.12(b) to show that each  $\rho_i$  must divide one of the  $\sigma_j$ , so that  $\rho_i = \epsilon\sigma_j$  for some unit  $\epsilon$ .
- (c) Prove, in (b), that  $k = l$  and that the primes  $\rho_i$  and  $\sigma_j$  can be paired so that each  $\rho_i$  is the product of  $\sigma_j$  and a unit.

**Exercise 2.14.** Suppose that  $\alpha = \delta^k$  for some positive integer  $k$  and for some  $\delta$  in  $I$  and that  $\alpha = \beta\gamma$ , where all the common divisors of  $\beta$  and  $\gamma$  are units. Prove that  $\beta$  and  $\gamma$  must both be  $k$ th powers, up to a unit factor.

### 7.3 The Equation $x^3 - 3y^3 = 1$

We apply the theory of the last section to show that  $x^3 - 3y^3 = 1$  has no solutions in integers except for  $(x, y) = (1, 0)$ . Writing the equation in the form  $x^3 - 1 = 3y^3$ , we can factor the left side over  $I$  and consider it as

$$(x - 1)(x - \omega)(x - \omega^2) = -\omega^2(1 - \omega)^2y^3 = -\omega^2(1 - \omega)^{3m+2}z^3,$$

where  $y = (1 - \omega)^m z$  for some nonnegative integer  $m$ , and  $z$  is in  $I$  and not divisible by  $1 - \omega$ .

#### Exercise 3.1.

- Verify that the difference of any two of  $x - 1$ ,  $x - \omega$ , and  $x - \omega^2$  is the product of  $1 - \omega$  and a unit.
- Prove that  $1 - \omega$  must divide at least one of the factors  $x - 1$ ,  $x - \omega$ , and  $x - \omega^2$ , and so it must divide each of the factors.
- Prove that a greatest common divisor of any pair of  $x - 1$ ,  $x - \omega$ , and  $x - \omega^2$  is  $1 - \omega$ .
- Prove that  $(1 - \omega)^2$  cannot divide more than one of  $x - 1$ ,  $x - \omega$ , and  $x - \omega^2$ .
- Prove that  $1 - \omega$  must divide  $y^3$ , so that  $m > 0$ .
- Prove that  $x - 1$ ,  $x - \omega$ , and  $x - \omega^2$  in some order have the forms  $\epsilon_1(1 - \omega)\gamma_1^3$ ,  $\epsilon_2(1 - \omega)\gamma_2^3$ , and  $\epsilon_3(1 - \omega)^{3m}\gamma_3^3$  for units  $\epsilon_i$  and numbers  $\gamma_i$  in  $I$  for which  $z$  is a unit times  $\gamma_1\gamma_2\gamma_3$  and where each  $\gamma_i$  is not divisible by  $1 - \omega$ .

#### Exercise 3.2.

- Verify that  $(x - 1) + \omega(x - \omega) + \omega^2(x - \omega^2) = 0$  and deduce that

$$\gamma_1^3 + \epsilon\gamma_2^3 = \zeta(1 - \omega)^{3m-1}\gamma_3^3 = 3\eta[(1 - \omega)^{m-1}\gamma_3]^3$$

for some units  $\epsilon$ ,  $\zeta$ , and  $\eta$ , where  $\gamma_1$ ,  $\gamma_2$ ,  $\gamma_3$  are the quantities of Exercise 3.1(f).

- Prove that  $\gamma_1$  and  $\gamma_2$  are each congruent to  $\pm 1$ , modulo  $(1 - \omega)$ , and deduce that for some choice of signs,  $\pm 1 \pm \epsilon \equiv 0 \pmod{(1 - \omega)^2}$ .
- Check the possibilities  $\pm 1$ ,  $\pm \omega$ ,  $\pm \omega^2$  of units and conclude that  $\epsilon \equiv \pm 1$ . ♠

By relabeling  $\gamma_2$  so that the minus sign is absorbed if necessary, we may assume that

$$\gamma_1^3 + \gamma_2^3 = 3\eta[(1 - \omega)^{m-1}\gamma_3]^3.$$

#### Exercise 3.3.

- By factoring  $\gamma_1^3 + \gamma_2^3 = (\gamma_1 + \gamma_2)(\gamma_1 + \omega\gamma_2)(\gamma_1 + \omega^2\gamma_2)$ , imitate the argument in Exercise 3.1 to show that  $m > 1$ .
- By iterating the process that takes us from  $x^3 - 1 = 3y^3$  to  $\gamma_1^3 + \gamma_2^3 = 3\eta[(1 - \omega)^{m-1}\gamma_3]^3$ , obtain by descent a succession of equations of the latter type involving lower positive powers of  $1 - \omega$  on the right. Deduce that the

assumption of a solution in  $I$  for  $x^3 + 1 = 3y^3$  must be false and that therefore  $x^3 - 3y^3 = 1$  has no nontrivial solution in ordinary integers.

**Exploration 7.1.** Extend the method of this section to prove that  $x^3 + y^3 = z^3$  cannot be solved in  $I$  and so the equation  $(u + 1)^3 = u^3 + v^3$  in Exercise 1.8 has no solution with  $(u, v) \neq (-1, 1), (0, 1)$ . Does  $x^3 - 2y^3 = 1$  have a solution with  $xy \neq 0$ ?

## 7.4 Obtaining the Cubic Version of Pell's Equation

Let  $c$  be any integer that is not a perfect cube, and let  $\theta$  be its real cube root. In Chapter 2 we noted that the quadratic Pell's equation could be written in terms of a norm function involving the square root of  $d$ . We can proceed the same way for the cubic case. The number  $\theta$  is the real root of the cubic equation

$$t^3 - c = 0.$$

This equation has three roots, namely  $\theta$ ,  $\theta\omega$ , and  $\theta\omega^2$ , where  $\omega$  is the imaginary cube root of unity,  $\frac{1}{2}(-1 + i\sqrt{3})$ .

Consider the expression  $x + y\theta + z\theta^2$ , where  $x$ ,  $y$ , and  $z$  are integers. We define its *norm* by

$$N(x + y\theta + z\theta^2) = (x + y\theta + z\theta^2)(x + y\theta\omega + z(\theta\omega)^2)(x + y\theta\omega^2 + z(\theta\omega^2)^2).$$

This will turn out to be a homogeneous polynomial of degree three in  $x$ ,  $y$ , and  $z$  with integer coefficients. The analogue of Pell's equation will therefore be

$$N(x + y\theta + z\theta^2) = k.$$

**Exercise 4.1.** Noting that  $\theta^3 = c$ ,  $\omega^2 + \omega + 1 = 0$ , and  $\omega^3 = 1$ , verify that  $N(x + y\theta + z\theta^2) = (x + y\theta + z\theta^2)[(x^2 - cyz) + (cz^2 - xy)\theta + (y^2 - xz)\theta^2] = x^3 + cy^3 + c^2z^3 - 3cxyz$ .

**Exercise 4.2.** Verify that  $N((x + y\theta + z\theta^2)(u + v\theta + w\theta^2)) = N(x + y\theta + z\theta^2) \cdot N(u + v\theta + w\theta^2)$ .

**Exercise 4.3.** Suppose that  $(x, y, z) = (u_1, v_1, w_1)$  is a solution of  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$ . For each positive integer  $n$ , we can expand  $(u_1 + v_1\theta + w_1\theta^2)^n$  in the form  $u_n + v_n\theta + w_n\theta^2$ , by making the reduction  $\theta^3 = c$ . From Exercise 4.2, argue that  $(u_n, v_n, w_n)$  is also a solution of  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$ .

**Exercise 4.4.** Observe that  $(x, y, z) = (1, 1, 1)$  is a solution of the equation  $x^3 + 2y^3 + 4z^3 - 6xyz = 1$ . Use Exercise 4.3 to derive other solutions of this equation in positive integers. Check these.

**Exercise 4.5.**

(a) Verify the factorization

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc).$$

(b) Use (a) to obtain the factorization

$$\begin{aligned} x^3 + cy^3 + c^2z^3 - 3cxyz \\ = \frac{1}{2}(x + y\theta + z\theta^2)((x - y\theta)^2 + (y\theta - z\theta^2)^2 + (x - z\theta^2)^2). \end{aligned}$$

(c) Deduce from (b) that if  $(x, y, z)$  is a triple of large positive integers that satisfy the equation  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$ , then  $x - y\theta$  and  $y - z\theta$  must be close to zero, so that  $x/y$  and  $y/z$  are approximations of  $\theta$ .**Exercise 4.6.** Let  $x, y$ , and  $z$  be integers. Use the factorization of Exercise 4.5(b) to show that  $(x + y\theta + z\theta^2)^{-1}$  has the form  $(p + q\theta + r\theta^2)/K$ , where  $p, q, r, K$  are all integers. Indeed, verify that

$$\begin{aligned} K &= x^3 + cy^3 + c^2z^3 - 3cxyz, \\ p &= x^2 - cyz, \\ q &= cz^2 - xy, \\ r &= y^2 - xz. \end{aligned}$$

**Exercise 4.7.** Note that if  $(u, v, w)$  is a solution of  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$ , then other solutions can be found from the expansion of negative integer powers of  $u + v\theta + w\theta^2$ . Use this to find solutions of  $x^3 + 2y^3 + 4y^3 - 6xyz = 1$  in integers, not all of which are positive.**Exercise 4.8.** So far, we have assumed that  $c$  is not a perfect cube. In this exercise we will see that when  $c = a^3$  for some integer  $a$ , the behavior is quite different.

(a) Verify that

$$\begin{aligned} 2(x^3 + a^3y^3 + a^6z^3 - 3a^3xyz) \\ = (x + ay + a^2z)[(x - ay)^2 + a^2(y - az)^2 + (a^2z - x)^2]. \end{aligned}$$

(b) Suppose that  $|a| \geq 2$  and that the integer triple  $(x, y, z)$  satisfies  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$ . Prove that  $y = az$  and deduce that  $x = a^2z \pm 1$ . What do you conclude about the set of solutions in this case?(c) Analyze the case  $|a| = 1$ .

## 7.5 Units

Let  $\mathbf{Q}(\theta)$  be the set of real numbers of the form  $u + v\theta + w\theta^2$ , where  $u, v, w$  are rational numbers and  $\theta^3$  is the integer  $c$ ;  $\mathbf{Z}(\theta)$  is the subset of  $\mathbf{Q}(\theta)$  for which



$u, v, w$  are integers. An element  $\epsilon$  of  $\mathbf{Z}(\theta)$  is called a *unit* if  $|N(\theta)| = 1$ . Since  $u^3 + cv^3 + c^2w^3 - 3cuvw = 1$  if and only if  $u + v\theta + w\theta^2$  is a unit, we begin our study of the cubic Pell's equation by looking at the structure of the units in  $\mathbf{Z}(\theta)$ . The treatment is similar to that of the quadratic case in Section 4.1.

**Exercise 5.1.**

- Verify that  $\mathbf{Q}(\theta)$  is a *field*; that is, the sum, difference, product, and quotient (with nonzero denominator) of two numbers in  $\mathbf{Q}(\theta)$  also belong to  $\mathbf{Q}(\theta)$ .
- Verify that  $\mathbf{Z}(\theta)$  is a *ring*; that is, the sum, difference, and product of two numbers in  $\mathbf{Z}(\theta)$  also belong to  $\mathbf{Z}(\theta)$ .
- Prove that if  $\alpha \in \mathbf{Z}(\theta)$ , then also  $N(\alpha)/\alpha \in \mathbf{Z}(\theta)$ .
- Show that an element  $\epsilon \in \mathbf{Z}(\theta)$  is a unit if and only if  $1/\epsilon \in \mathbf{Z}(\theta)$ . (Cf. the definition of unit in Section 7.2.)
- Show that if  $\epsilon$  and  $\eta$  are units, then so is  $\epsilon\eta$ .

**Exercise 5.2.**

- Let  $u + v\theta + w\theta^2 \in \mathbf{Q}(\theta)$ . Define

$$\begin{aligned}\tau_1(u + v\theta + w\theta^2) &= u + v\omega\theta + w\omega^2\theta^2, \\ \tau_2(u + v\theta + w\theta^2) &= u + v\omega^2\theta + w\omega\theta^2,\end{aligned}$$

where  $\omega$  is an imaginary cube root of 1. Prove that for  $\alpha, \beta \in \mathbf{Q}(\theta)$  and  $i = 1, 2$ ;

$$\tau_i(\alpha \pm \beta) = \tau_i(\alpha) \pm \tau_i(\beta), \quad \tau_i(\alpha\beta) = \tau_i(\alpha)\tau_i(\beta), \quad \tau_i(1/\alpha) = 1/\tau_i(\alpha).$$

(These equations specify that  $\tau_1$  and  $\tau_2$  are *isomorphisms* of  $\mathbf{Q}(\theta)$  into the field of complex numbers. The norm of an element  $\alpha$  is the product  $\alpha \cdot \tau_1\alpha \cdot \tau_2\alpha$ .)

- Verify that  $\tau_1(\alpha)$  is the complex conjugate of  $\tau_2(\alpha)$  for  $\alpha \in \mathbf{Q}(\theta)$ .
- Verify that if  $\alpha = u + v\theta + w\theta^2$ , then  $\alpha, \tau_1(\alpha)$ , and  $\tau_2(\alpha)$  are the three roots of the cubic equation

$$t^3 - 3ut^2 + 3(u^2 - cvw)t - (u^3 + cv^3 + c^2w^3 - 3cuvw) = 0$$

with rational coefficients. Observe that if  $\alpha \in \mathbf{Z}(\theta)$ , then the cubic polynomial has integer coefficients.

**Exercise 5.3.** Determine all units  $\epsilon \in \mathbf{Z}(\theta)$  whose absolute values  $|\epsilon|$  are equal to 1.

**Exercise 5.4.** Let  $E$  be the set of units in  $\mathbf{Z}(\theta)$  and suppose that  $E$  contains elements other than 1 and  $-1$ .

- Let  $M$  be a positive number exceeding 1. Prove that there are at most finitely many elements  $\epsilon$  of  $E$  for which  $1 \leq |\epsilon| \leq M$ .
- Prove that  $E$  contains a smallest element  $\gamma$  that exceeds 1.
- Let  $\epsilon \in E$ ,  $|\epsilon| \neq 1$ . Suppose that  $\delta$  is the element among  $\epsilon, -\epsilon, 1/\epsilon$ , and  $-1/\epsilon$  that exceeds 1. Prove that  $\delta = \gamma^m$  for some positive integer  $m$ . Deduce that  $\epsilon = \pm\gamma^n$  for some integer  $n$ . ♠

We turn to the question of the existence of a nontrivial unit whenever  $c$  is not a cube. The basic approach is similar to that used for the quadratic case in Section 4.2. From Exercise 4.1, we recall that

$$N(x + y\theta + z\theta^2) = (x + y\theta + z\theta^2)[(x^2 - cyz) + (cz^2 - xy)\theta + (y^2 - xz)\theta^2].$$

The strategy is to first show that for some real number  $M$ ,  $N(x + y\theta + z\theta^2) \leq M$  occurs for infinitely many triples  $(x, y, z)$ , so that  $N(x + y\theta + z\theta^2)$  must assume some value infinitely often.

**Exercise 5.5.** Let  $n$  be an arbitrary positive integer and let the indices  $i$  and  $j$  satisfy  $-n \leq i, j \leq n$ .

- (a) Explain why for each of the  $(2n + 1)^2$  possible choices of the pair  $i, j$  we can select an integer  $a_{ij}$  for which  $0 \leq a_{ij} + i\theta + j\theta^2 < 1$ .
- (b) Use the pigeonhole principle to argue that for some positive integer  $k$  not exceeding  $4n^2$ , there are two distinct pairs of indices  $(i, j)$  for which the corresponding numbers  $a_{ij} + i\theta + j\theta^2$  fall in the same interval

$$\left\{ t : \frac{k-1}{4n^2} \leq t \leq \frac{k}{4n^2} \right\}.$$

- (c) Deduce from (b) that there are integers  $u, v, w$ , not all zero, for which  $|v| \leq 2n$ ,  $|w| \leq 2n$ , and  $|u + v\theta + w\theta^2| \leq 1/4n^2 \leq 1/k(v, w)^2$ , where  $k(v, w) = \max(|v|, |w|)$ . (Note that  $k(v, w) \geq 1$ .)
- (d) Use the fact that

$$u + v\omega\theta + w\omega^2\theta^2 = (u + v\theta + w\theta^2) + v(\omega - 1)\theta + w(\omega^2 - 1)\theta^2$$

to show that

$$\left| u + v\omega\theta + w\omega^2\theta^2 \right| \leq \frac{1}{k(v, w)^2} + 4k(v, w)|c| \leq 5k(v, w)|c|$$

and prove that

$$\left| N(u + v\theta + w\theta^2) \right| \leq 25c^2.$$

- (e) Prove that there are infinitely many triples  $(u, v, w)$  of integers for which  $|N(u + v\theta + w\theta^2)| \leq 25c^2$ .
- (f) Prove that there exists a positive integer  $m$  for which  $N(x + y\theta + z\theta^2) = m$  has infinitely many solutions, with  $x, y, z$  integers.

**Exercise 5.6.** Let  $m$  be the positive integer found in Exercise 5.5.

- (a) Prove that there are two distinct triples  $(u_1, v_1, w_1)$  and  $(u_2, v_2, w_2)$  of integers such that

$$N(u_1 + v_1\theta + w_1\theta^2) = N(u_2 + v_2\theta + w_2\theta^2) = m$$

and

$$u_1 \equiv u_2, \quad v_1 \equiv v_2, \quad w_1 \equiv w_2,$$

modulo  $m$ .

(b) Suppose that

$$m \left[ \frac{u_1 + v_1\theta + w_1\theta^2}{u_2 + v_2\theta + w_2\theta^2} \right] = u_3 + v_3\theta + w_3\theta^2.$$

Prove that  $u_3, v_3, w_3$  are integers each divisible by  $m$ .

(c) Let  $u = u_3/m, v = v_3/m$ , and  $w = w_3/m$ . Verify that  $(u, v, w)$  is a triple of integers distinct from  $(1, 0, 0)$  for which  $N(u + v\theta + w\theta^2) = 1$ . This establishes that  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$  is always solvable nontrivially for integers when the parameter  $c$  is not a cube.

## 7.6 Matrix and Vector Considerations

As for the quadratic Pell's situation, we induce from the multiplication of  $u + v\theta + w\theta^2$  and  $x + y\theta + z\theta^2$  a corresponding  $*$ -multiplication for triples  $(u, v, w)$  and  $(x, y, z)$  by

$$(u, v, w) * (x, y, z) = (ux + cvz + cwy, uy + vx + cwz, uz + vy + wx).$$

Let  $(u, v, w)^{-1}$  be the triplet that corresponds to  $(u + v\theta + w\theta^2)^{-1}$ . If we think of  $(u, v, w)$  as being a fixed multiplier, we can describe its effect in matrix-vector form by

$$M \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ux + cwy + cvz \\ vx + uy + cwz \\ wx + vy + uz \end{pmatrix},$$

where  $M$  is the  $3 \times 3$  matrix

$$\begin{pmatrix} u & cw & cv \\ v & u & cw \\ w & v & u \end{pmatrix}.$$

For  $n$  an integer, let  $(u, v, w)^n = (u_n, v_n, w_n)$  if  $(u + v\theta + w\theta^2)^n = u_n + v_n\theta + w_n\theta^2$ .

Setting  $g_c(u, v, w) = u^3 + cv^3 + c^2w^3 - 3cuvw$ , we define  $(u, v, w)^0 = (1, 0, 0)$ ,

$$(u, v, w)^{-1} = \left( \frac{u^2 - cvw}{g_c(u, v, w)}, \frac{cw^2 - uv}{g_c(u, v, w)}, \frac{v^2 - uw}{g_c(u, v, w)} \right)$$

(cf. Exercise 4.1), and

$$(u, v, w)^{-n} = [(u, v, w)^{-1}]^n.$$

Suppose now that  $g_c(x, y, z) = 1$  has solutions other than  $(x, y, z) = (1, 0, 0)$  and that  $(x, y, z) = (u, v, w)$  is the solution for which  $u + v\theta + w\theta^2$  has the smallest positive value exceeding 1 (the fundamental solution). Then by Exercise 5.4, the entire set of solutions is given by  $(x, y, z) = (u_n, v_n, w_n) = (u, v, w)^n$ ,

where  $n$  is an integer. As in the quadratic case, we can find recursions satisfied by each of the sequences  $\{u_n\}$ ,  $\{v_n\}$ , and  $\{w_n\}$ .

The sum of two  $3 \times 3$  matrices and the product of a number and a matrix are defined componentwise as was done for  $2 \times 2$  matrices in Section 1.2. The product of two  $3 \times 3$  matrices is given by

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \\ = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21}+a_{13}b_{31} & a_{11}b_{12}+a_{12}b_{22}+a_{13}b_{32} & a_{11}b_{13}+a_{12}b_{23}+a_{13}b_{33} \\ a_{21}b_{11}+a_{22}b_{21}+a_{23}b_{31} & a_{21}b_{12}+a_{22}b_{22}+a_{23}b_{32} & a_{21}b_{13}+a_{22}b_{23}+a_{23}b_{33} \\ a_{31}b_{11}+a_{32}b_{21}+a_{33}b_{31} & a_{31}b_{12}+a_{32}b_{22}+a_{33}b_{32} & a_{31}b_{13}+a_{32}b_{23}+a_{33}b_{33} \end{pmatrix}.$$

Note that in the exercises,  $M$  is the matrix defined above and  $g_c(u, v, w) = 1$ .

**Exercise 6.1.** Let

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Verify that for any  $3 \times 3$  matrix  $A$ ,  $AI = IA = A$ .

**Exercise 6.2.** Verify that

$$\begin{aligned} u_{n+1} &= uu_n + cvv_n + cvw_n, \\ v_{n+1} &= vu_n + uv_n + cww_n, \\ w_{n+1} &= wu_n + vv_n + uw_n. \end{aligned}$$

**Exercise 6.3.**

(a) Define

$$M^{-1} = \begin{pmatrix} u^2 - cvw & cv^2 - cuw & c^2w^2 - cuv \\ cw^2 - uv & u^2 - cvw & cv^2 - cuw \\ v^2 - uw & cw^2 - uv & u^2 - cvw \end{pmatrix}.$$

Verify that this definition is appropriate in that  $MM^{-1} = M^{-1}M = I$ .

(b) Verify that

$$M^2 = \begin{pmatrix} u^2 + 2cvw & 2cuw + cv^2 & 2cuv + c^2w^2 \\ 2vu + cw^2 & 2cvw + u^2 & cv^2 + 2cuw \\ 2wu + v^2 & cw^2 + 2uv & 2cvw + u^2 \end{pmatrix}.$$

(c) Verify that

$$M^2 - 3uM + 3(u^2 - cvw)I - M^{-1} = 0$$

and deduce that

$$M^3 - 3uM^2 + 3(u^2 - cvw)M - I = 0.$$

(d) Verify that

$$M \begin{pmatrix} \theta^2 \\ \theta \\ 1 \end{pmatrix} = (u + v\theta + w\theta^2) \begin{pmatrix} \theta^2 \\ \theta \\ 1 \end{pmatrix}.$$

(e) Use (c) to deduce that the sequences  $\{u_n\}$ ,  $\{v_n\}$ , and  $\{w_n\}$  each satisfy the recursion

$$x_{n+3} = 3ux_{n+2} - 3(u^2 - cvw)x_{n+1} + x_n.$$

**Exercise 6.4.** In Exercise 4.4, the solution  $(x, y, z) = (1, 1, 1)$  was given for  $g_2(x, y, z) = 1$ . Determine  $(1, 1, 1)^{-1}$  and use the recursion in Exercise 6.3(e) to derive other solutions. Check these.

**Exercise 6.5.**

(a) Verify that  $g_3(x, y, z) = 1$  can be rewritten as

$$(x^3 - 1) + 3y^2 + 9(z^2 - xy)z = 0.$$

- (b) Deduce that for any solution of (a),  $x \equiv 1$  and  $y \equiv 0$  modulo 3. Use these facts to obtain a solution by inspection.
- (c) Determine other solutions by taking \*-powers and check that the sequence of solutions you get satisfies the recursion in Exercise 6.3(e).

## 7.7 Solutions for Special Cases of the Parameter $c$

As in our initial investigation of the quadratic Pell's equation, it is possible to find solutions for

$$g_c(x, y, z) \equiv x^3 + cy^3 + c^2z^3 - 3cxyz = 1 \quad (1)$$

quite readily for certain values of  $c$ . This section will examine some ways of doing this.

**Exercise 7.1.**

(a) One strategy for locating a solution is to try  $x = 1$ . Then  $y$  and  $z$  must satisfy

$$y^3 + cz^3 - 3yz = 0. \quad (2)$$

Verify that if (2) is to be satisfied, then

$$c = \frac{-y(y^2 - 3z)}{z^3} = \frac{y(3z - y^2)}{z^3}.$$

Use this fact to determine values of  $c$  for which (2) has solutions with  $z = 1$  and for which (1) has a solution with  $x = z = 1$ .

- (b) Determine values of  $c$  for which (1) has a solution with  $x = 1, z = -1$ .
- (c) Determine values of  $c$  for which (1) has a solution with  $x = 1, z = \pm 2, \pm 3$ .

- (d) Make a table of some of these solutions  $(x, y, z)$  along with the inverse solutions  $(x, y, z)^{-1}$  as defined in Section 7.6.

**Exercise 7.2.** Suppose that  $c = -d$ . Prove that  $(x, y, z) = (u, v, w)$  is a solution of  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$  if and only if  $(x, y, z) = (u, -v, w)$  is a solution of  $x^3 + dy^3 + d^2z^3 - 3dxyz = 1$ . Thus, in analyzing Pell's equation, we can get the whole story essentially by looking at positive values of  $c$ .

**Exercise 7.3.**

- (a) Suppose  $c = k^3 + r$  where  $k$  and  $r$  are integers. Let  $s$  satisfy  $rs = 3k$ . Verify that  $(x, y, z) = (1, ks, -s)$  is a solution of (1).
- (b) The formula in (a) will always generate a *rational* solution for (1). Verify that for  $c = 29$ , a solution is  $(x, y, z) = (1, 27/2, -9/2)$ .
- (c) We can specialize to  $k = rt$ ,  $s = 3t$  in (a), so that  $c = r^3t^3 + r$  and  $(x, y, z) = (1, 3rt^2, -3t)$  is a solution. List all of the positive values less than 300 for which we can find a solution in this way along with the corresponding solutions and inverse solutions.
- (d) Specialize to the case that  $r$  is a multiple of 3 and obtain solutions for further values of  $c$ .
- (e) Are there any other positive values of  $c$  not exceeding 100 for which we may obtain solutions? Try letting  $k$  be other than an integer.

**Exercise 7.4.** Consider the equation

$$x^3 + cy^3 + c^2z^3 - 3cxyz = 8, \quad (3)$$

where  $c = a^3 + 2a$ .

- (a) Verify that this equation is satisfied by  $(x, y, z) = (2, 3a, -3)$ .
- (b) By considering  $(2 + 3a\theta - 3\theta^2)^2$ , deduce and check that

$$(x, y, z) = (4 - 18ac, 12a + 9c, -12 + 9a^2)$$

is a solution of

$$x^3 + cy^3 + c^2z^3 - 3cxyz = 64. \quad (4)$$

- (c) Show that when  $a = 2b$  is even, the values of  $x, y, z$  in (b) are divisible by 4. In this case, verify that  $c = 4b(2b^2 + 1)$  and that

$$(x, y, z) = (1 - 36b^2(2b^2 + 1), 3b(6b^2 + 5), 3(3b^2 - 1))$$

satisfies (1).

- (d) Determine a solution of (1) in positive integers when  $c = 12, 72$ , and  $228$ .

**Exercise 7.5.**

- (a) Suppose that  $c = r^2$ . Prove that  $(x, y, z) = (u, v, w)$  satisfies

$$x^3 + cy^3 + c^2z^3 - 3cxyz = 1$$

if and only if  $(x, y, z) = (u, rw, v)$  satisfies

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1.$$

- (b) Verify that  $(x, y, z) = (4, 3, 2)$  satisfies (1) when  $c = 3$  and use this result to obtain a solution to (1) when  $c = 9$ .
- (c) Exercise 7.1 gave a method of solving equation (1) for  $c = 5$ . Use this solution to generate a solution  $(x, y, z)$  for which  $y$  is divisible by 5. From this, deduce a solution to (1) for  $c = 25$ .

**Exercise 7.6.**

- (a) Suppose that  $c = r^3s$ . Prove that  $(x, y, z) = (u, v, w)$  is a solution to

$$x^3 + cy^3 + c^2z^3 - 3cxyz = 1$$

if and only if  $(x, y, z) = (u, rv, r^2w)$  is a solution to

$$x^3 + sy^3 + s^2z^3 - 3sxyz = 1.$$

- (b) Find a solution in integers to the equation

$$x^3 + 16y^3 + 256z^3 - 48xyz = 1.$$

**Exercise 7.7.** Consider solutions of (1) with  $z = 0$ . In this case, the equation simplifies to  $x^3 + cy^3 = 1$ . With reference to Section 7.1, determine values of  $c$  for which a solution of this type is available along with some solutions and their inverses.

**Exercise 7.8.** Investigate solutions of  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$  in the special cases that  $c = k^3 \pm 1$  and  $c = k^3 \pm 3$ , and see whether you can find solutions that depend algebraically on the parameter  $k$ .

**Exercise 7.9.**

- (a) Verify that

$$g_c(x + cz, x + y, y + z) = (c + 1)g_c(x, y, z).$$

- (b) Starting with the fact that  $g_c(1, 0, 0) = 1$ , use (a) to determine at least two solutions to  $g_c(x, y, z) = 1$  in positive rationals. Are there any situations in which integer solutions can be found in this way?
- (c) Is one of the two solutions found in (b) a power of the other?

**Exploration 7.2.** Are there any values of  $c$  for which  $g_c(x, y, z) = 1$  does *not* have a solutions with  $x = 1$ ?

## 7.8 A Procedure That Often, but Not Always, Works

As seen in Exercise 1.5(b), when  $x, y, z$  are large positive integers, then  $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$  implies that  $x$  is close to  $y\theta$  and  $y$  is close to  $z\theta$ . This

suggests that we generate triple of integers  $(x, y, z)$  with these properties and hope that some of them will give us a solution. We start with four triples for which the signs of  $x^3 - cy^3$  and  $y^3 - cz^3$  together cover all four possibilities. Let  $p = \lfloor \theta \rfloor$ , the largest integer whose cube is less than  $c$ ; let  $q = \lfloor p\theta \rfloor$  and  $r = \lfloor (p+1)\theta \rfloor$ .

We form a table that begins

$(x, y, z)$	$x^3 - cy^3$	$y^3 - cz^3$
$(q, p, 1)$	—	—
$(q+1, p, 1)$	+	—
$(r, p+1, 1)$	—	+
$(r+1, p+1, 1)$	+	+

From this seed, we proceed as follows: Suppose the final entry in the table so far is  $(u, v, w)$ . Let  $(u', v', w')$  be that last of the previous entries for which

$$u^3 - cv^3 \quad \text{and} \quad u'^3 - cv'^3$$

have opposite signs and also

$$v^3 - cw^3 \quad \text{and} \quad v'^3 - cw'^3$$

have opposite signs. The next entry is  $(u + u', v + v', w + w')$ .

Thus, the fifth entry in the table will have  $(x, y, z) = (q + r + 1, 2p + 1, 2)$ . The hope is that adding triples with opposite signs will keep bringing  $x^3 - cy^3$  and  $y^3 - cz^3$  relatively close to zero and so, in due course, make  $x^3 + cy^3 + cz^3 - 3cxyz = 1$ . Surprisingly, this works quite often; more surprisingly, it does not work all the time.

**Exercise 8.1.** For  $c = 2$ , verify that the algorithm yields the following table:

$(x, y, z)$	$x^3 - 2y^3$	$y^3 - 2z^3$	$x^3 + 2y^3 + 4z^3 - 6xyz$
(1, 1, 1)	—	—	1
(2, 1, 1)	+	—	2
(2, 2, 1)	—	+	4
(3, 2, 1)	+	+	11
(4, 3, 2)	+	+	6
(5, 4, 3)	—	+	1
(7, 5, 4)	+	—	9
(12, 9, 7)	+	+	22
(13, 10, 8)	+	—	5

Continue the table to generate more solutions to  $x^3 + 2y^3 + 4z^3 - 6xyz = 1$ , but check that the algorithm does not pick up  $(x, y, z) = (281, 223, 177)$ .



**Exercise 8.2.** For  $c = 5$ , verify that the algorithm yields

$(x, y, z)$	$x^3 - 5y^3$	$y^3 - 5z^3$	$x^3 + 5y^3 + 25z^3 - 15xyz$
(1, 1, 1)	−	−	16
(2, 1, 1)	+	−	2
(3, 2, 1)	−	+	8
(4, 2, 1)	+	+	9
(5, 3, 2)	−	−	10
(9, 5, 3)	+	−	4

Continue this table until a solution to  $x^3 + 5y^3 + 25z^3 - 15xyz = 1$  is found.

**Exercise 8.3.** Try the algorithm to obtain solutions to

$$x^3 + cy^3 + c^2z^3 - 3cxyz = 1$$

when  $c = 3, 4, 6, 7, 9, 10, 11, 12, 13, 14$ . For the cases  $c = 6, 10, 11, 13$ , a pocket calculator is especially useful, and for the case  $c = 12$ , a programmable calculator or computer is desirable.

**Exercise 8.4.**

(a) The smallest positive solution of

$$x^3 + 15y^3 + 225z^3 - 45xyz = 1$$

is  $(x, y, z) = (5401, 2190, 888)$ . Check this solution and verify that the algorithm fails to find it.

(b) The smallest positive solution of

$$x^3 + 16y^3 + 256z^3 - 48xyz = 1$$

is  $(x, y, z) = (16001, 6350, 2520)$ . Check this solution and verify that the algorithm fails to find it.

**Exercise 8.5.** If you have suitable computational power at your disposal, check the efficacy of the algorithm for higher values of  $c$ .

## 7.9 A More General Cubic Version of Pell's Equation

So far, we have examined Pell's equation in the form  $N(x + y\theta + z\theta^2) = 1$ , where  $\theta$  is a root of the special equation  $t^2 - c = 0$ . We extend our investigation to equations derived from roots of the cubic equation

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

where  $a, b$ , and  $c$  are arbitrary integers. Suppose that the cubic polynomial cannot be factored as a product of polynomials of lower degree with integer coefficients and that its roots are  $\theta = \theta_1, \theta_2$ , and  $\theta_3$  with  $\theta$  real. Define

$$g(x, y, z) = (x + y\theta_1 + z\theta_1^2)(x + y\theta_2 + z\theta_2^2)(x + y\theta_3 + z\theta_3^2).$$

The analogue of Pell's equation is  $g(x, y, z) = 1$ .

**Exercise 9.1.** Recall that  $a = -(\theta_1 + \theta_2 + \theta_3)$ ,  $b = \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3$ , and  $c = -\theta_1\theta_2\theta_3$ . Show that

$$g(x, y, z) = x^3 - cy^3 + c^2z^3 - ax^2y + (a^2 - 2b)x^2z + bxy^2 + acy^2z \\ + (b^2 - 2ac)xz^2 - bcyz^2 + (3c - ab)xyz.$$

**Exercise 9.2.** Let  $\theta$  be a root of the equation  $t^3 = t + 1$ .

(a) Verify that

$$g(x, y, z) = x^3 + y^3 + z^3 + 2x^2z + xz^2 - xy^2 - yz^2 - 3xyz.$$

- (b) It turns out to be uncommonly easy to find solutions of  $g(x, y, z) = 1$ . By inspection, see how many you can get.
- (c) We can obtain all solutions as  $*$ -powers of a fixed one  $(u, v, w)$ , where  $u + v\theta + w\theta^2$  has the smallest value exceeding 1. Do this.
- (d) Using matrix techniques, determine a recursion satisfied by the sequence of solutions.

**Exercise 9.3.** Let  $\theta$  be a root of the equation  $t^3 - 7t^2 + 14t - 7 = 0$ .

- (a) Verify that  $g(x, y, z) = x^3 + 7y^3 + 49z^3 + 7x^2y + 21x^2z + 14xy^2 + 49y^2z + 98xz^2 + 98yz^2 + 77xyz$ .
- (b) Determine some solutions of  $g(x, y, z) = 1$  with  $z = 0$ .
- (c) Determine some solutions of  $g(x, y, z) = 1$  with  $x = z = 1$ .
- (d) List other solutions. Do you think that they are all obtainable as  $*$ -powers of a single solution?

## 7.10 More Explorations

**Exploration 7.3.** Consider the function  $g_2(x, y, z) = x^3 + 2y^3 + 4z^3 - 6xyz$ . There appear to be a number of interesting regularities that occur, as, for example, in the following table:

$n$	$(x, y, z)$	$g_2(x, y, z)$
0	(1, 0, 0)	1
1	(1, 1, 0)	3
2	(1, 1, 1)	1
3	(3, 2, 2)	3
4	(5, 4, 3)	1
5	(11, 9, 7)	3

If  $(x_n, y_n, z_n)$  is the  $n$ th triple, then  $\{x_n\}$ ,  $\{y_n\}$ , and  $\{z_n\}$  each appear to satisfy the recursion

$$t_{2m} = t_{2m-1} + t_{2m-2} + t_{2m-3}, \\ t_{2m+1} = 2t_{2m} + t_{2m-2},$$

for  $m \geq 2$ .

Another table of regularities is

$n$	$(x, y, z)$	$g_2(x, y, z)$
0	(1, 0, 0)	1
1	(0, 1, 0)	2
2	(1, -1, 1)	9
3	(0, 0, 1)	4
4	(1, 0, 1)	5
5	(1, 1, 1)	1
6	(2, 1, 1)	2
7	(1, 2, 1)	9
8	(2, 2, 1)	4
9	(3, 3, 2)	5
10	(5, 4, 3)	1

In this case, the recursion seems to be, for  $m \geq 1$ ,

$$t_{5m-1} = t_{5m-3} + t_{5m-4},$$

$$t_{5m} = t_{5m-1} + t_{5m-4},$$

$$t_{5m+1} = t_{5m} + t_{5m-5},$$

$$t_{5m+2} = t_{5m} + t_{5m-4},$$

$$t_{5m+3} = t_{5m+1} + t_{5m-4}.$$

It seems to happen more frequently than one would expect that

$$g_2(x_1, y_1, z_1) + g_2(x_2, y_2, z_2) = g_2(x_1 + x_2, y_1 + y_2, z_1 + z_2).$$

For example,

$$g_2(1, 1, 1) + g_2(5, 4, 3) = g_2(6, 5, 4),$$

$$g_2(5, 4, 3) + g_2(8, 6, 5) = g_2(13, 10, 8),$$

$$g_2(1, 1, 0) + g_2(1, 1, 1) = g_2(2, 2, 1),$$

$$g_2(1, 0, 0) + g_2(3, 3, 2) = g_2(4, 3, 2).$$

Can anything be said in general?

**Exploration 7.4.** Let  $c$  be a noncubic integer and  $\theta$  its real cube root. The number  $x + y\theta + z\theta^2$  in  $\mathbf{Q}(\theta)$  is an algebraic integer if and only if it is a root of a monic polynomial with integer coefficients. The monic cubic polynomial whose roots are  $x + y\theta + z\theta^2, x + y\omega\theta + z\omega^2\theta^2, x + y\omega^2\theta + z\omega\theta^2$  is  $t^3 - pt^2 + qt - r$  where  $p = 3x, q = 3(x^2 - cyz)$ , and  $r = x^3 + cy^3 + c^2z^3 - 3cxyz$ . Now,  $p, q, r$  are certainly integers when  $x, y, z$  are themselves integers. Are there values of  $c$  for which algebraic integers exist where  $x, y, z$  are not all (ordinary) integers, but  $p, q, r$  are integers?

## 7.11 Notes

Section 3. For an account of  $\mathbf{Q}(\sqrt{-3})$ , consult G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers* (Oxford), Chapter XIII. In the fourth edition (1960), the relevant material is found on pages 188–189 and 192–196. This chapter gives a treatment of a few special cases of Fermat’s “theorem” that there are no nontrivial solutions in integers of  $x^n + y^n = z^n$  when  $n$  is a positive integer exceeding 2. This is the theorem that was finally settled by Andrew Wiles in the last decade of the twentieth century.

5.5–5.6. See G.B. Mathews, *On the Arithmetic Theory of the Form  $x^3 + ny^3 + n^2z^3 - 3nxyz$* , *Proc. London Mathematical Society* 21 (1890), 280–287.

7.9. When  $x, y, z$  are positive and  $g_c(x, y, z) = 1$ , then  $y/z, x/y$ , and  $cz/x$  are approximations to  $c^{1/3}$  whose product is  $c$ . Thus some are over- and others under-approximations. We can add numerators and denominators to get better approximations  $(x+y)/(y+z), (x+cz)/(y+x)$ . We select the third approximation to make the product of the three to be equal to  $c$ :  $c(y+z)/(x+cz)$ . This motivates the transformation

$$S(x, y, z) = (x + cz, y + x, z + y).$$

Compare the values of  $g_c(x + cz, y + x, z + y)$ ,  $g_c(cz, x, y)$ , and  $g_c(x, y, z)$ .

The transformation is related to the following algorithm for determining the cube root of any positive number  $c$ . Begin with the quadruple  $(1, 1, 1, c)$ . We form a sequence of quadruples in which  $(p, q, r, cp)$  is followed by  $(p + q, q + r, r + cp, c(p + q))$ . It turns out that as one proceeds along the sequence,  $q/p, r/q, cp/r$  all approach  $c^{1/3}$ . This can be generalized to higher roots. Thus, for the  $k$ th root of  $c$ , start with  $(1, 1, 1, \dots, 1, c)$  (with  $k$  ones) and apply the transformation

$$(p, q, r, \dots, s, cp) \longrightarrow (p + q, q + r, \dots, s + cp, c(p + q)),$$

where each of the first  $k$  entries is the sum of the corresponding entry and its successor in the previous vector.

Section 9. A recent researcher who has done a significant amount of work on the determination of cubic fields is T.W. Cusick; an example of the work of him and his colleagues is listed in the bibliography.

## 7.12 Hints

2.2. Let  $\phi(x + y\omega) = x + y\omega^2$ , the surd conjugate of  $x + y\omega$ . Show that  $\phi(r) = r$  for each rational  $r$ ,  $\phi(\alpha \pm \beta) = \phi(\alpha) \pm \phi(\beta)$ ,  $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ . Note that  $N(\alpha) = \alpha\phi(\alpha)$ .

2.10. Since  $\sigma|\rho$ ,  $\rho = \sigma\epsilon$  for some algebraic integer  $\epsilon$ . Since  $\rho|\sigma$ , deduce that  $\epsilon^{-1}$  must also be an algebraic integer.

2.12(b). Note that  $\mu = \xi\alpha\mu + \eta\beta\mu$  and that  $\beta$  divides each term on the right side.

3.2(b). Let  $\gamma_1 = r_1 + s_1\omega = (r_1 + s_1) - s_1(1 - \omega)$  and note that  $r_1 + s_1$  is not divisible by  $3 = (1 - \omega)(1 - \omega^2)$ .

5.1(a). Use the fact that  $\theta^3 = c$  to check products and refer to Exercise 1.7 to show that the reciprocal of an element in  $\mathbf{Q}(\theta)$  is also in  $\mathbf{Q}(\theta)$ .

5.1(d). Observe that if  $\alpha \in \mathbf{Z}(\theta)$ , then  $N(\alpha)$  must be an integer. Use the fact that  $N(1/\alpha) = 1/N(\alpha)$ .

5.2(c). Determine the coefficients by looking at the sum, sum of products of pairs, and products of the roots. Use the fact that  $\omega^3 = 1$  and  $\omega + \omega^2 = -1$ .

5.4(a). Observe that  $\tau_1(\epsilon)$  and  $\tau_2(\epsilon)$  are complex conjugates and use the fact that  $\epsilon\tau_1(\epsilon)\tau_2(\epsilon) = 1$  to determine bounds for  $|\tau_1(\epsilon)|$  and  $|\tau_2(\epsilon)|$ . Now use the symmetric functions of  $\epsilon$ ,  $\tau_1(\epsilon)$ , and  $\tau_2(\epsilon)$  to find bounds for the coefficients of  $\epsilon$  (cf. Exercise 5.2(b)).

5.5(c). Take the difference of the numbers in the pair found in (b).

5.5(e). Select  $(u_1, v_1, w_1)$  such that  $N(u_1 + v_1\theta + w_1\theta^2) \leq 25|c|^2$ . Determine an integer  $n$  such that  $1/4n^2 < |u_1 + v_1\theta + w_1\theta^2|$ , and use (c) to find a distinct triple  $(u_2, v_2, w_2)$  with  $N(u_2 + v_2\theta + w_2\theta^2 \equiv 2) \leq 25c^2$ . Continue on in this way, churning out an infinite sequence of triples.

5.6(a). Note that there are only finitely many equivalence classes, modulo  $m$ , available for the triple  $(u, v, w)$ . Use the pigeonhole principle.



<http://www.springer.com/978-0-387-95529-2>

Pell's Equation

Barbeau, E.J.

2003, XII, 212 p., Hardcover

ISBN: 978-0-387-95529-2