CHAPTER TEN

DIOPHANTINE EQUATIONS

§1. NORM FORMS

Let $p(x)$ be a monic irreducible polynomial of degree n with integer coefficients, and suppose that θ is a root of the polynomial. This polynomial has n distinct roots, $\theta_1 = \theta$, θ_2, $\cdots$, θ_n; suppose that s of the roots, θ_i with $1 \leq i \leq s$ are real and that $2t$, θ_i with $s+1 \leq i \leq s+2t$ of them are nonreal, the nonreal roots consisting of t complex conjugate pairs, $(\theta_{s+j}, \theta_{s+t+j})$, with $1 \leq j \leq t$. Thus, $n = s + 2t$.

The field $\mathbf{Q}[\theta]$, generated by the rationals with θ adjoined, has a vector basis $\{1, \theta, \theta^2, \cdots, \theta^{n-1}\}$. The natural isomorphism

$$x_0 + x_1\theta + \cdots + x_{n-1}\theta^{n-1} \longrightarrow (x_0, x_1, \cdots, x_{n-1})$$

of $\mathbf{Q}[\theta]$ onto $\mathbf{Q}^n$ induces a product $\{(\cdots, x_i, \cdots) * (\cdots, y_i \cdots) = (\cdots, z_i, \cdots)$, where $(\sum x_i\theta^i)(\sum y_i\theta^i) = (\sum z_i\theta^i)$. We have n distinct field isomorphisms from $\mathbf{Q}[\theta]$ into $\mathbf{C}$ via $\theta \to \theta_i$, s of which are real valued and $2t$ of which take some nonreal values.

An *algebraic integer* is any complex number that is a zero of a monic polynomial with integer coefficients. An algebraic integer ϵ is a *unit* if and only if its multiplicative inverse ϵ^{-1} is also an algebraic integer. Two algebraic integers α and β are *associates* if there exists a unit ϵ for which $\alpha = \epsilon\beta$.

The function

$$f(\mathbf{x}) = \prod_{i=1}^{n}(x_0 + x_1\theta_i + \cdots + x_{n-1}\theta_i^{n-1}) \tag{1}$$

(with $\mathbf{x} = (x_0, x_1, x_2, \cdots, x_{n-1})$) is a polynomial in n variables x_0, $\cdots$, x_{n-1} with real coefficients known as a *norm form*, its value being the norm $N(\xi)$ of the element $\xi = x_0 + x_1\theta + \cdots + x_{n-1}\theta^{n-1}$ in the field extension $\mathbf{Q}(\theta)$ of $\mathbf{Q}$. We wish to study the Diophantine equation $f(\mathbf{x}) = \pm 1$. It turns out that the set of its solutions is a group with respect to the $*$ product. If $\mathbf{x}$ is a solution of this equation, then the element $x_0 + x_1\theta + \cdots + x_{n-1}\theta^{n-1}$ is a *unit* in the ring $\mathbf{Z}(\theta)$; these are the elements of the ring whose multiplicative inverses also lie in the ring.

A simple example of an equation of this type is *Pell's equation* $x^2 - dy^2 = \pm 1$, where d is a nonsquare integer, as the left side can be factored as $(x + \sqrt{d}y)(x - \sqrt{d}y)$, $\sqrt{d}$ being a root of the irreducible polynomial $x^2 - d$.

A key result is the Dirichlet Unit Theorem:

Dirichlet Unit Theorem; *There exists a set of units $\{\epsilon_1, \cdots, \epsilon_r\}$, where $r = s + t - 1$ such that every unit ϵ in $\mathbf{Z}(\theta)$ can be written uniquely in the form*

$$\epsilon = \zeta\epsilon_1^{k_1}\epsilon_2^{k_2}\cdots\epsilon_r^{k_r}\ ,$$

where ζ is a root of unity and each ϵ_i is a unit of infinite order.

A sketch of the proof of this result will be given. We begin by describing a *vector lattice.* Let $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_m\}$ be a linearly independent set of vectors in a real vector space of dimension $n \geq m$. The set of vectors of the form $\sum_i a_i\mathbf{e}_i$, where $a_i \in \mathbf{Z}$ is a vector lattice. The lattice is *full* when $m = n$. Two linearly independent sets $E = \{\mathbf{e}_i\}$ and $F = \{\mathbf{f}_i\}$ give the same vector lattice if and only if they are related by a linear transformation $\mathbf{F} = C\mathbf{E}$ where the transformation matrix C has determinant with absolute value 1. When the vector space is given a topology defined by the inner product with respect to the basis, the lattice generated by the basis is a discrete set. Indeed, any discrete subgroup of the vector space is a lattice. The *fundamental parallelepiped* of the lattice is the set $T \equiv \{\sum_i u_i \mathbf{e}_i : 0 \leq u_i < 1\}$. The translates $T + \mathbf{z}$, where $\mathbf{z}$ belongs to the lattice are pairwise disjoint sets and there are only finitely many of them that intersect any ball $B(\mathbf{0}, r)$ of radius r centered at the origin.

Let M be the $\mathbf{Z} -$ *module* in $\mathbf{C}$ consisting of numbers of the form $\xi = x_0 + x_1\theta + \cdots + \cdots + x_{n-1}\theta^{n-1}$, where each x_i is an integer, and let $\xi_i = x_0 + x_1\theta_i + \cdots + x_{n-1}\theta_i^{n-1}$ be the ith *associate* of ξ. This module can be coordinatized through its associates as $(\xi_1, \xi_2, \cdots, \xi_s, \xi_{s+1}, \cdots, \xi_{s+t})$ for $\xi \in M$, where each ξ_i $(1 \leq i \leq s)$ is real and each ξ_j is nonreal (with two real coordinates) for $s + 1 \leq j \leq t$. The linear space M has an inner product whose norm is given by

$$\|\xi\|^2 = \xi_1^2 + \cdots + \xi_s^2 + |\xi_{s+1}|^2 + \cdots + |\xi_t|^2 \ .$$

For each $\eta \in M$, the mapping $\alpha \longrightarrow \eta\alpha$ maps M linearly into itself with determinant $N(\eta)$.

M can be embedded in a $n-$dimensional real vector space $L^{s,t}$ consisting of vectors

$$\mathbf{x} = (x_1, x_2, \cdots, x_s, x_{s+1}, \cdots, x_{s+t})$$

where x_i is real if $1 \leq i \leq s$ and x_{s+j} is complex (with a real and imaginary part) if $1 \leq j \leq t$. We give $L^{s,t}$ norms that extends the vector norm on M by assigning an inner product that specifies $\|\mathbf{x}\|$ as the square root of $\sum_{i=1}^s x_i^2 + \sum_{j=1}^t |x_{s+j}|^2$ and extends the "algebraic" norm $N(\mathbf{x}) = x_1 x_2 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2$. The set $S \equiv \{\mathbf{x} \in L^{s,t} : N(\mathbf{x}) = 1\}$ is closed under multiplication, defined coordinatewise, of two vectors in $L^{s,t}$.

Consider the vector space $\mathbf{R}^{s+t}$. We define the logarithmic mapping L from $L^{s,t}$ into $\mathbf{R}^{s+t}$ by

$$L(\mathbf{x}) = (\log|x_1|, \log|x_2|, \cdots, \log|x_s|, \log|x_{s+1}|^2, \cdots, \log|x_{s+t}|^2) \ .$$

Observe that $L(\mathbf{xy}) = L(\mathbf{x}) + L(\mathbf{y})$, so that L maps the multiplicative structure of $L^{s,t}$ to the additive structure of $\mathbf{R}^{s,t}$. The set $\{\mathbf{x} : N(\mathbf{x}) = 1\}$ is mapped by L onto the $(s + t - 1)-$dimensional subspace V of $\mathbf{R}^{s+t}$ consisting of those vectors whose components sum to 0. The kernel of L in $L^{s,t}$ consists of vectors all of whose components have absolute value 1 and so it is bounded.

On M, this mapping L takes the form

$$L(\xi) = (\log|\xi_1|, \log|\xi_2|, \cdots, \log|\xi_s|, \log|\xi_{s+1}|^2, \log|\xi_{s+2}|^2, \cdots, \log|\xi_{s+t}|^2) \ .$$

Let E be the set of units contained in M and U be the set of those that lie in the kernel of L. U contains all the roots of unity that happen to be in M, in particular ± 1, so that U is nontrivial. In fact, U contains only roots of unity. If $\alpha \in U$, then all powers of α belong to the bounded set U; accordingly, there can be only finitely many of them, from which we deduce that some power of α must equal 1. Thus, U, containing the group $\{1, -1\}$ of order 2, is a finite cyclic group of even order and consists only of the roots of unity in M.

Since the norm of any number of E is equal to ± 1, the sum of the entries l_i of $L(\xi)$ for any ξ satisfies $\sum_i l_i = 0$, so that $L(E)$ lies in a subspace of dimension $s + t - 1$. It remains to show that $L(E)$ is full in the subspace of $\mathbf{R}^{s+t}$ of vectors for which the sum of the entries is 0.

To show that the lattice is full, we use the criterion that *a lattice N contained in an inner product linear space V is full if and only if there is a bounded set S such that V is contained in the union $S + N$ of its translates by elements of N*. If the lattice is full, S can be the fundamental parallelepiped. If the lattice is not full, let S be any bounded set. Then there is a number r for which $\|x\| < r$ for all $x \in S$. Since the subspace W generated by N is proper in V, we can find $y \in V$ orthogonal to W for which $\|y\| > r$. Suppose if possible that $y = u + z$ with $u \in S$ and $z \in N$. Then

$$\|y\|r < \|y\|^2 = \langle y, y \rangle = \langle y, u \rangle \leq \|y\|\|u\| < \|y\|r \ ,$$

which is a contradiction.

A result needed to finish the proof of Dirichlet's Theorem is the following:

Minkowski Theorem on Convex Bodies. *Let J be a full lattice in $\mathbf{R}^n$ whose fundamental parallelepiped has volume Δ, and let X be a bounded, centrally symmetric convex set with volume Γ. If $\Gamma > 2^n\Delta$, then X contains at least one nonzero point of J.*

Proof. Note that, if a bounded set Y is such that its translates $Y_z = Y + z$ for $z \in J$ are pairwise nonintersecting, then the volume of Y is less than Δ. To see this, note that, where T is the fundamental parallelepiped,

$$\text{Vol }(Y) = \sum\{\text{Vol }(Y \cap T_{-z}) : z \in J\} = \sum\{\text{Vol }(Y_z \cap T) : z \in J\} \ ,$$

where the right sum computes the volume of the union of finitely many disjoint subsets of T and therefore must be less than Vol $(T) = \Delta$.

The volume of the set $\frac{1}{2}X$ obtained from X by a dilatation of factor $1/2$ exceeds Δ. Hence, two of its translates by elements of J must intersect, so that there exist elements $x_1, x_2 \in X$ and $z_1, z_2 \in J$ so that $z_1 \neq z_2$ and $\frac{1}{2}x_1 + z_1 = \frac{1}{2}x_2 + z_2$. Hence

$$z_1 - z_2 = \frac{1}{2}(-x_1) + \frac{1}{2}(x_2) \in X \ .$$

and the result follows. □

To relate all of this to M, consider the coordinatization of M with respect to its associates (ξ_j), where $\xi_j = \eta_j + \zeta_j i$ for $s+1 \leq j \leq t$ where η_j and ζ_j are real. If X is the bounded set of points ξ for which $|\xi_i| < c_i$ $(1 \leq i \leq s)$ and $|\xi_j|^2 < c_j$ $(s+1 \leq j \leq s+t)$, then the volume of X is

$$\int_{-c_1}^{c_1} d\xi_1 \cdots \int_{-c_s}^{c_s} d\xi_s \int_{\eta_{s+1}^2+\zeta_{s+1}^2<c_{s+1}} d\eta_{s+1} d\zeta_{s+1} \cdots \int_{\eta_{s+t}^2+\zeta_{s+t}^2<c_{s+t}} d\eta_{s+t} d\zeta_{s+t} = 2^s \pi^t c_1 \cdots c_{s+t} \ .$$

Noting that $n = s + 2t$, we obtain from Minkowski's theorem that if the fundamental parallelepiped of the full lattice M has volume Δ and if $c_1c_2 \cdots c_{s+t} > (4/\pi)^t\Delta$, then there is a nonzero element ξ of M for which

$$|\xi_1| < c_1, \cdots, |\xi_s| < c_s, |\xi_{s+1}|^2 < c_{s+1}, \cdots, |\xi_t|^2 < c_t \ .$$

With this background, we return to the task of proving Dirichlet's Theorem by showing that $L(E)$ is full in the $(s+t-1)-$dimensional subspace V of $\mathbf{R}^{s+t}$ by constructing a bounded set in $L^{s,t}$ and then using the mapping L to obtain a bounded subset of $\mathbf{R}^{s+t}$ whose translates by elements of $L(E)$ cover V.

With $S = \{\mathbf{x} \in L^{s,t} : N(\mathbf{x}) = 1\}$, let y be an arbitrary point of $M \cap S$. Then M and yM are two lattices whose fundamental parallelepipeds havs the same volume Δ. Select real numbers $c_1, \cdots, c_t$ for which $c \equiv c_1c_2 \cdots c_{s+t} > (4/\pi)^t\Delta$. Let

$$X = \{\mathbf{x} \in L^{s,t} : |x_i| < c_i(1 \leq i \leq s), |x_{s+j}|^2 < c_{s+j}(1 \leq j \leq t)\} \ .$$

By Minkowski's theorem applied to the lattice yM, X contains a nonzero point $x = y\alpha$ where α is a nonzero element of M. We have that $N(\alpha) = N(\mathbf{x}) < c$.

Since at most finitely many pairwise nonassociate elements of M have norm less than c, we can find elements α_1, α_2, $\cdots$, α_m to one of which any element of norm less than c is associated. Thus, there is a unit ϵ for which $\alpha\epsilon = \alpha_h$ for some $h \leq m$. Then $y = x\alpha^{-1} = (x\alpha_h^{-1})\epsilon$.

Let $Z = S \cap (\cup\{X\alpha_h^{-1} : 1 \leq h \leq m\})$. Z is bounded since each $X\alpha_h^{-1}$ is bounded and $y \in Z\epsilon$ for some unit ϵ. Since y and ϵ both belong to S, then $x\alpha_h^{-1} = y\epsilon^{-1}$ belong to S and hence to Z. Thus $S \subset \cup\{Z\epsilon : \epsilon \text{ a unit in } M\}$.

Apply the map L. Since Z is a bounded subset, $L(Z)$ is also bounded and $V = \cup\{L(Z) + L(\epsilon) : \epsilon \text{ a unit in } M\}$. Dirichlet's theorem follows.

§2. A CUBIC EXAMPLE

Let θ be a root of the equation $x^3 = x + 1$, The corresponding norm form is

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

Since the equation $x^3 = x + 1$ has one real and two nonreal roots $((s, t) = (1, 1))$, the solutions of $g(x) = 1$ have the structure of a cyclic group. Three obvious solutions are $(x, y, z) = (1, 0, 0), (0, 1, 0), (0, 0, 1)$, which correspond to the elements 1, θ and θ^2 in $\mathbf{Q}[\theta]$.

The set of elements in $\mathbf{Z}[\theta]$ that correspond to solutions of $g(x) = 1$ is a group that is closed under multiplication by θ. Since $(x + y\theta + z\theta^2)\theta = z + (x + z)\theta + y\theta$, if (x, y, z) satisfies $g(x, y, z) = 1$, then so also does $(z, x + z, y)$. The transformation $(x, y, z)^{\mathbf{t}} \longrightarrow (z, x + z, y)^{\mathbf{t}}$ is implemented by the matrix

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \ ,$$

which satisfies the equation $M^3 = M + 1$. It follows from this that the sequence of solutions $\mathbf{x}_n = M^n(1, 0, 0)^{\mathbf{t}}$ satisfies the recursion $\mathbf{x}_n = \mathbf{x}_{n-2} + \mathbf{x}_{n-3}$.

We obtain a bilateral sequence of solutions

$$\{\cdots, (0, -1, 1), (1, 1, -1), (-1, 0, 1), (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (0, 1, 1), (1, 1, 1), (1, 2, 1), \cdots \ .$$

If we define the sequence $\{u_n\}$ by the recursion, $u_0 = 1$, $u_1 = u_2 = 0$ and $u_n = u_{n-2} + u_{n-3}$ for every integer n, then $(x, y, z) = (u_n, u_{n+2}, u_{n+1})$ satisfies $g(x, y, z) = 1$.

§3. PELL'S EQUATION

Pell's equations arise from the norm form for the real nth primitive root of unity. In the quadratic case, it is the familiar $x^2 - dy^2 = \pm 1$, where d is a nonsquare integer. When $d < 0$, then this has finitely many solutions, which all arise from roots of unity in $\mathbf{Q}(\sqrt{-d})$. When $d > 0$, then it has infinitely many solutions (x_m, y_m) arising from $x_m + y_m\sqrt{d} = (u + v\sqrt{d})^m$, where $u + v\sqrt{d}$ is a "fundamental" unit in $\mathbf{Z}(\sqrt{d})$.

In fact, $(x_m, y_m) = (T_m(u), U_m(u)v)$ where T_m and U_m are Chebyshev polynomials of the first and second types. (See Section 5.4.) To see this, observe that $dv^2 = u^2 - 1$ and that

$$\begin{aligned}(T_m(u) + U_m(u)v\sqrt{d})(u + v\sqrt{d}) &= (uT_m(u) + (u^2 - 1)U_m(u)) + (T_m(u) + uU_m(u))v\sqrt{d} \\ &= T_{m+1}(u) + U_{m+1}(u)v\sqrt{d} \ .\end{aligned}$$

The cubic version of Pell's equation is

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

where c is an integer not equal to a perfect cube. By Dirichlet's theorem, the set of solutions is, up to roots of unity, a cyclic group; they can be found by taking powers of a fundamental unit $u + v\theta + w\theta^2$, where θ is the real cube root of c.

The sequence of solutions generated by (u,v,w) is defined by the recursion $(x_{m+1}, y_{m+1}, z_{m+1})^{\mathbf{t}} = M(x_m, y_m, z_m)^{\mathbf{t}}$, where the transition matrix

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

has characteristic polynomial $\lambda^3 - 3u\lambda^2 + 3(u^2 - cvw)\lambda - 1 = 0$. Thus, $\{x_m\}$, $\{y_m\}$ and $\{z_m\}$ each satisfy the recursion

$$t_{m+1} = 3ut_m - 3(u^2 - cvw)t_{m-1} + t_{m-2} \ .$$

Example 10.1. When $c = 2$, the fundamental solution of $x^3 + 2y^3 + 4z^3 - 6xyz = 1$ is $(1,1,1)$, the recursion is $t_{m+1} = 3t_m + 3t_{m-1} + t_{m-2}$ and the sequence of solutions is

$$\{\cdots, (-1,1,0), (1,0,0), (1,1,1), (5,4,3), (19,15,12), (73,58,46), \cdots\} \ .$$

Example 10.2. When $c = 3$, the fundamental solution of $x^3 + 3y^3 + 9z^3 - 9xyz = 1$ is $(4,3,2)$, the recursion is $t_{m+1} = 12t_m + 6t_{m-1} + t_{m-2}$ and the sequence of solutions is

$$\{\cdots, (4,3,-4), (-2,0,1), (1,0,0), (4,3,2), (52,36,25), \cdots\} \ .$$

The quartic version of Pell's equation, obtained from calculating the norm of $x + y\theta + z\theta^2 + w\theta^3$, where θ is a fourth root of c, is given by

$$(x^2 + cz^2 - 2cyw)^2 - c(2xz - y^2 - cw^2)^2 = \pm 1 \ .$$

When $c < 0$, then the equation $t^4 - c = 0$ has two pairs of complex conjugates roots, and so the set of solutions of this equation is essentially a cyclic group. When $c > 0$ and c is not a square, then the set of solutions is essentially a free group on two generators (up to roots of unity). If we write $X = x^2 + cz^2 - 2cyw$ and $Y = 2xz - y^2 - cw^2$, then it appears as though the two generators will yield $(X,Y) = (1,0)$ and (X,Y) a fundamental solution of $X^2 - cY^2 = \pm 1$. It would be nice to find a nice representation for the set of solutions.

The quintic Pells's equation is the rather formidable looking

$$\begin{aligned}(x^5 + cy^5 + c^2z^5 + c^3u^5 + c^4v^5) - 5c(x^3yv + x^3zu + xy^3z) - 5c^2(y^3uv + xz^3v + yz^3u + xyu^3) \\ - 5c^3(zu^3v + xuv^3 + yzv^3) + 5c(x^2y^2u + x^2yz^2) \\ + 5c^2(x^2u^2v + x^2zv^2 + xy^2v^2 + xz^2u^2 + y^2z^2v + y^2zu^2) \\ + 5c^3(yu^2v^2 + z^2uv^2) - 5c^2(xyzuv) = \pm 1 \ .\end{aligned}$$

In this case, $s = 1$, $t = 2$, so that the group of solutions is essentially free with two generators.

The sixth degree Pell's equation has the form

$$p^2 - cq^2 = r^3 + cs^3 + c^2t^3 - 3crst = \pm 1$$

where

$$\begin{aligned} p = {} & x^3 + (3xu^2 + 3y^2v + z^3 - 3xyw - 3xvz - 3uyz)c \\ & + (v^3 + 3zw^2 - 3uvw)c^2 \ , \end{aligned}$$

$$\begin{aligned} q = {} & (3x^2u + y^3 - 3xyz) \\ & + (u^3 + 3yv^2 + 3z^2w - 3xvw - 3uyw - 3uvz)c + w^3c^2 \ , \end{aligned}$$

$$r = x^2 + 2czv - cu^2 - 2cyw \ ,$$

$$s = 2xz + cv^2 - y^2 - 2cuw \ ,$$

and

$$t = z^2 + 2xv - 2yu - cw^2 \ .$$

When c is positive and not a cube, there are two real and two nonreal complex conjugate pairs of sixth roots of c, so that the group of solutions is essentially free with three generators. There are four types of solutions, those for which

$$(p,q) = (\pm 1, 0) \qquad (r,s,t) = (\pm 1, 0, 0)$$

$$(p,q) = (\pm 1, 0) \qquad (r,s,t) \ \text{ nontrivial}$$

$$(p,q) \ \text{ nontrivial} \qquad (r,s,t) = (\pm 1, 0, 0)$$

and both (p,q) and (r,s,t) nontrivial.

For example, when $c = 2$, we have solutions $[(x,y,z,u,v,w),(p,q),(r,s,t),\pm 1]$ given by

$$[(1,1,0,0,0,0),(1,1),(1,-1,0),-1]$$

$$[(1,0,0,1,0,0),(7,5),(-1,0,0),-1]$$

$$[(1,0,1,0,1,0),(1,0),(5,4,3),+1]$$

$$[(3,2,2,2,2,2),(3,2),(1,0,0),+1]$$

$$[(11,10,9,8,7,6),(3,2),(5,4,3),+1]$$

$$[(145,138,126,108,90,78),(1,0),(1,0,0),+1]$$

§4. POLYNOMIAL VERSION OF PELL'S EQUATION

In solving Pell's equation $x^2 - dy^2 = 1$ for various values of d, it can be observed that some solutions follow a pattern when d has a certain character and at other times, the solution for a given d can be quite idiosyncratic. Thus, when $d = t(t+1)$ for some positive integer t, $x^2 - dy^2 = 1$ is satisfied by $(x,y) = (2t+1, 2)$.

Sometime the search for a solution of $x^2 - dy^2 = 1$ can be shortened by solving $x^2 - dy^2 = k$ where k is one of -1, 4 and -4. For, if $-1 = u^2 - dv^2 = N(u + v\sqrt{d})$, then $1 = N((u + v\sqrt{d})^2) = (u^2 + dv^2)^2 - d(2uv)^2$. Suppose $u^2 - dv^2 = \pm 4$. If u and v are both even, then $(x,y) = (u/2, v/2)$ will satisfy $x^2 - dy^2 = \pm 1$, while if both u and v are odd, then an integer solution will be provided from $\frac{1}{8}(u + v\sqrt{d})^3$.

We can formulate finding solutions of $x^2 - dy^2 = k$ that follow a pattern in terms of solving a polynomial version of Pell's equation, where d, x and y are polynomials in one or more variables. The following table gives some examples of such polynomials d and corresponding solutions.

$d(t)$	k	$x(t), y(t)$
$t^2 - 1$	1	$(t, 1)$
$t^2 + 1$	-1	$(t, 1)$
$t^2 \pm 2$	1	$(t^2 \pm 1, t)$
$t^2 \pm 4$	∓ 4	$(t, 1)$
$t(t \pm 1)$	1	$(2t \pm 1, 2)$
$t(4t \pm 1)$	1	$(8t \pm 1, 4)$
$t(9t \pm 2)$	1	$(9t \pm 1, 3)$
$t(9t \pm 4)$	4	$(9t \pm 2, 3)$
$3(3t^2 \pm 4)$	4	$(3t^2 \pm 2, t)$
$9t^2 \pm 8t + 2$	1	$((9t \pm 4)^2 + 1, 3(9t \pm 4))$
$49t^2 \pm 20t + 2$	1	$((49t \pm 10)^2 - 1, 7(49t \pm 10))$
$3(3t^2 \pm 1)$	1	$(6t^2 \pm 1, 2t)$
$t(t^3 \pm 2)$	1	$(t^3 \pm 1, t)$
$t(s^2t \pm 1)$	1	$(2s^2t \pm 1, 2s)$
$t(s^2t \pm 2)$	1	$(s^2t \pm 1, s)$
$t(s^2t \pm 4)$	4	$(s^2t \pm 2, s)$

In a similar way, we can find polynomial solutions for $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$ for certain polynomials $c(t)$. For example,

$c(t)$	$(x(t), y(t), z(t))$
$t^3 \pm 1$	$(1, \pm 3t^2, \mp 3t)$
$t^3 \pm 1$	$(t^2, t, 1)$
$t^3 \pm 1$	$(\mp t, \pm 1, 0)$
$t^3 \pm t$	$(1, \pm 3t, \mp 3)$
$t^3 \pm 3$	$(1, \pm t^2, \mp t)$
$8k^3 \pm 2$	$(1, \pm 6t^2, \mp 3t)$

For the quartic $(x^2 + cz^2 - 2cyw)^2 - c(2xz - y^2 - cw^2)^2 = 1$, we have the examples

$c(t)$	$(x(t), y(t), z(t), w(t))$
$t^4 \pm 1$	$(2t^4 \pm 1, 2t^3, 2t^2, 2t)$
$t^4 \pm 1$	$(t^3, t^2, t, 1)$
$t^4 \pm 2$	$(t^4 \pm 1, t^3, t^2, t)$
$t^4 \pm t$	$(2t^3 \pm 1, 2t^2, 2t, 2)$
$t^4 \pm 2t$	$(t^3 \pm 1, t^2, t, 1)$
$s^4t^4 \pm 2t$	$(s^4t^3 \pm 1, s^3t^2, s^2t, s)$

§4. INVESTIGATIONS

1. **Pell's equations: fundamental solutions.** For the standard Pell's equation of degree 2, there is a robust algorithm for determining the fundamental solution. Algorithms that might be used for Pell's equation of higher degree are more hit or miss; they may turn up solutions that may or may not be fundamental, or may not lead anywhere at all. Furthermore, Dirchlet's theoreml gives us information about the algebraic structure of the set of solutions, but there is much more to be investigated. When the degree of the Pell's equation is composite, we can see in the cases of 4 and 6 that there exists a natural mapping of solutions to solutions of lower degree equations. For Pell's equation of degree 4, it appears that the set of solutions has two generators, one of which maps to the solution $(1, 0)$ of the

corresponding quadratic Pell's equation and the other to a nontrivial solution of the quadratic equation. Need this nontrivial solution be fundamental? What happens for the sixth degree equation, when the solution set has three generators.

It might be particularly instructive to look at the situation where the parameter c is equal to 2, since the determining of solutions seems to be more amenable.

References

1. Edward J. Barbeau, *Pell's equation.* Springer, 2003

2. Z.I. Borevich & I.R. Shafarevich, *Number theory.* Academic, 1966. Chapter 2.