CUBIC PELL EQUATION

A mathematical vignette

Ed Barbeau, Toronto, ON

The setting

The theory of the usual Pell's equation $x^2 - dy^2 = 1$, where d is a nonsquare positive integer is built on the fact that the left side is the norm of the quadratic integer $x + y\sqrt{d}$, namely

$$x^2 - dy^2 = (x + y\sqrt{2})(x - y\sqrt{2}) = N(x + \sqrt{2}).$$

The second factor is the second root of the irreducible quadratic equation $t^2 - 2xt + (x^2 - dy^2) = 0$. The set of soluion of $x^2 - dy^2 = 0$ is the sequence (x_n, y_n) given by

$$x^n + y^n\sqrt{2} = (x_1 + y_1\sqrt{2})^n,$$

where (x_1, y_1) is the smallest or *fundamental* solution of $x^2 - dy^2 = 1$

There is a similar situation at the cubic level. Suppose that d is a noncubic integer and that θ is its real cube root. For integers x, y and z, the number $x + y\theta + z\theta^2$ is the root of a cubic equation with integer coefficients whose other roots are $x + y\omega\theta + z\omega^2\theta^2$ and $x + y\omega^2\theta + z\omega\theta^2$. The norm $g_d(x, y, z)$ of this number is defined to be the product of the three roots:

$$\begin{aligned} g_d(x,y,z) &= (x + y\theta + z\theta^2)(x + y\omega\theta + z\omega^2\theta^2)(x + y\omega^2\theta + z\omega\theta^2) \\ &= (x + y\theta + z\theta^2)(x^2 + \theta y^2 + \theta^2 z^2 - xy\theta - yz - xz\theta^3) \\ &= \tfrac{1}{2}(x + y\theta + z\theta^2)[(x - y\theta)^2 + (y\theta - z\theta^2)^2 + (x - z\theta^2)^2] \\ &= x^3 + dy^3 + d^2z^3 - 3dxyz. \end{aligned}$$

The cubic analogue of Pell's equation is

$$g_d(x, y, z) = 1.$$

Since $g_{-d}(x, y, z) = g_d(x, -y, z)$, every solution of the cubic Pell's equation for $d > 0$ corresponds to one for $d < 0$, so there is no loss of generality in assuming that $d > 0$.

The norm of the product of two numbers of the form $x + y\theta + z\theta^2$ is the product of the norms, so that just as in the quadratic situation, we can use the quantity $x + y\theta + z\theta^2$ to generate a bilaeral sequence of solutions to $g_d(x, y, z) = 1$:

$$(x_n + y_n + z_n) = (x + y\theta + z\theta^2)^n$$

where n is an integer and (x, y, z) is the *fundamental* solution (apart from $(1, 0, 0)$) in smallest positive integers. (That there is a single generator is a consequence of the Dirichlet unit theorem.)

Solving $g_d(x, y, z) = 1$ depends on finding the fundamental solution. In the case of the quadratic equation, there is an algorithm that involves continued fractions that does this. However, in the cubic equation there seems to be no such systematic process and ad hoc methods and brute force computations are necessary. Some of the fundamental solutions are pretty large.

Let S be bilateral sequence of solutions. The product

$(x+y\theta+z\theta^2)*(u+v\theta+w\theta^2) = (xu+dyw+dzv)+(xv+yu+dzw)\theta+(xw+yv+zu)\theta^2$

induce an operation of S,

$$(x, yz) * (u, v, w) = (xu + d(yw + zv), xv + yu + dzw, xw + yv + zu)$$

, that makes S a cyclic group with identity $(1, 0, 0)$. We have that

$$g_d((x, y, z) * (u, v, w)) = g_d(x, y, z)g_d(u, v, w).$$

As a side comment, we note that $(x, y, z)^{-1}$ and $z, y, x)$ are orthogonal vectors.

The inverse of (x, y, z) is equal to

$$(x^2 - dyz, dz^2 - xy, y^2 - xz).$$

The fundamental solution

One strategy is suppose that a solution has a special form and then hunt for values of d for which such a solution exists. Another is to check the situation for special values of d that exhibit a pattern.

1. Can one of the variables vanish? x must be nonzero, for otherwise the left side of $g_d(x, y, z)$ is divisible by d. If $yz = 0$, then we are looking for solutions of $x^3 + dy^3 = 1$ where $c = -d$ or $c = -d^2$.

If $y = \pm 1$, then it is straightforward to find that, when $d = r^3 \pm 1$, $(x, y) = (r, \pm 1)$ satisfies the equation.

Thus, we have the solutions for $g_d(x, y, z) = 1$:

$$(d; x, y, z, 0) = (r^3 - 1; r, -1, 0), (r^3 + 1, -r, 1, 0)$$

and the inverse solutions

$$(d; x, y, z, 0) = (r^3 \pm 1; r^2, r, 1).$$

For $y = \pm 3$, we get

$$(d; x, y, 0) = (19; -8, 3, 0), (37; 10, -3, 0), (182; -17, 3, 0), (254; 10, -3, 0),$$
$$(651; -26, 3, 0), (813; 28, -3, 0), (1588; -35, 3, 0), (1876; 37, -3, 0).$$

There are also other isolated examples with smaller numbers:

$$(d; x, y) = (17; 18, -7), (20; -19, 7), (1727; -71, 6), (1801; 73, -6), (635; 361, -42).$$

(These examples are drawn from a list in the article *Computation of soutions of* $x^3 + Dy^3 = 1$ by H.C. Williams and R. Holte in *Math. of Computation* 31:139 (July, 1977), 778-785.)

The examples for $y = \pm 2, \pm 3$ can be identified as part of a regular patterns:

$$\begin{aligned}(d; x, y, 0) &= (64r^3 - 24r^2 + 3r; (-8r + 1, 2, 0);\\ (d; x, y, 0) &= (64r^3 + 24r^2 + 3r; 8r + 1, -2, 0);\\ (d; x, y, 0) &= (27r^3 - 9r^2 + r; -9r + 1, 3, 0);\\ (d; x, y, 0) &= (27r^3 + 9r^2 + r; 9r + 1, 3, 0).\end{aligned}$$

More generally, we have

$$\begin{aligned}(d; x, y, 0) &= (r^6 - 3r^3 + 3; -r^3 + 1, r, 0);\\ (d; x, y, 0) &= (r^6 + 3r^3 + 3; r^3 + 1, -r, 0);\\ (d; x, y, 0) &= (s^3r^6 - 3s^2r^3 + 3s; -sr^3 + 1, r, 0);\\ (d; x, y, 0) &= (s^3r^6 + 3s^2r^3 + 3s; sr^3 + 1, -r, 0).\end{aligned}$$

In the case of $r = 6$, there are more possibilities:

$$\begin{aligned}(d; (x, y, 0) &= (1728r^6 - 72r^3 + 1; -72r + 1, 6, 0);\\ (d; (x, y, 0) &= (1728r^6 + 72r^3 + 1; 72r + 1, -6, 0).\end{aligned}$$

In addition, there are some solutions that do fall into a these patterns:

$$\begin{aligned}(d; x, y, 0) = (17; 18, -7, 0), (20; -19, 7), (635; 361, -42), (5080; 361, -21, 0)\\ (17145; 361, -14, 0), (18745; 1036, -34, 0), (32006; -127, 14)\\ (32042; 667, -21, 0), (48949; 4097, -112, 0)\end{aligned}$$

If $x^3 + dy^3 = 1$, then $-dy^3 = (x - 1)(x^2 + x + 1)$. Suppose that $x - 1 = r^3$. If $x = r^3 + 1$, then $x^2 + x + 1 = r^6 + 3r^3 + 3$. We can then take $d = r^6 + 3r^3 + 3$ and $y = -r$, so we obtain

$$(d; x, y, 0) = (r^6 + 3r^3 + 3; r^3 + 1, -r, 0).$$

This approach can be modified when $x^3 - 1$ has a cubic factor r^3 other than $x - 1$. For example $x^3 - 1$ is divisible by 8 when $x \equiv 1 \pmod 8$. If $x = 9r + 1$, then this generates the solutions

$$(d; x, y, z) = 64r^2 + 24r + 3; 8r + 1, -2, 0) \qquad (d : x, y, z) + (64r^2 - 24r + 3; -8r + 1, 2, 0).$$

If $x^3 - 1$ is divisible by 27, then x has one of the form $9r + 1$, and we get

$$(d; x, y, z) = (27r^2 + 9r + 1; 9r + 1, -3, 0) \qquad (d; x, y, z) = (27r^2 - 9r + 1; -9r + 1; 3).$$

2. Another option is to look for solutions in which $x = 1$. In this case, the equation reduces to

$$y^3 + dz^3 - 3yz = 0,$$

whereupon

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

If $z = 1$, then a positive value whose square is less that 3 corresponds to a positive value of d, as does any negative value of y whose square exceeds 3. This leads to the cases:

$$(d; x, y, z) = (2; 1, 1, 1);$$
$$(d; x, y, z) = (r(r^2 - 3); 1, -r, 1) \qquad (k \geq 2).$$

Similarly, when $z = -1$, we are led to

$$(d; x, y, z) = (r(r^2 + 3); 1, r, -1).$$

If $z = 2$, then $d = y(6 - y^2)/8 = (-y)(y^2 - 6)/8$, from which $-y$ must be a multiple of 8. This yields

$$(d; x, y, z) = (r(8r^2 - 3); 1, -4k, 2).$$

Similarly, when $z = -2$, we are led to

$$(d; x, y, z) = (r(8r^2 + 3); 1, 4k, -2).$$

Trying $z = \pm 3$ and $z = \pm 4$ provides

$$(d; x, y, z) = (r(r^2-1); 1, -3r, 3), (r(r^2+1); 1, 3r, -r), (r(64r^2-3); (1, -16r, 4), (r(64r^2+3); 1, 16r, -40.$$

These suggest the more general

$$(d; x, y, z) = (r(r^2s^3 - 3); 1, -rs^2, s), (r(r^2s^3 + 3; 1, rs^2, -s).$$

In particular, when $r = 1$, we get

$$(d; x, y, z) = (s^3 - 3; 1, -s^2, s), (s^3 + 3; 1, s^2, -s).$$

An alternative route is to begin with $g_d(1, ks, -s) = 1$ when $d = k^3 + r$, provided that $3k = rs$. The most obvious cases where r divides $3k$ are $r = \pm 1, \pm 3, \pm 3k$, as well as $s = 3t$ when $k = rt$. These yields the possibilities for solutions:

d	Solution	Inverse of solution
$k^3 + 1$	$(1, 3k^2, -3k)$	
$k^3 - 1$	$(1, -3k^2, 3k)$	
$k^3 + 3$	$(1, k^2, -k)$	
$k^3 - 3$	$(1, -k^2, k)$	
$k^3 + 3k$	$(1, k, -1)$	
$k^3 - 3k$	$(1, -k1)$	
$r^3t^3 + r$	$(1, 3rt^2, -3t)$	
$r^3t^3 - r$	$(1, -3rt^2, 3t)$	

3. The solutions of the equation for d and d^2 are related. We have that (u, v, w) satisfies $g_{d^2}(u, v, w) = 1$ if and only if $(u, dw.v)$ satisfies $g_d(u, v, w) = 1$. The correspondence between the solution $(d^2 : u, v, w)$ and $(d : u, dw, v)$ is carried over to products of such corresponding solutions with respect to $*$.

Thus, every solution for the parameter d^2 gives rise to a solution for the parameter d. However, not every solution $(d; x, y, z)$ has y divisible by d, and so will not generate a solution for the parameter d^2. However, it can be shown (by looking at the products of the fundamental solution modulo d) that some power of the fundamental solution will have the value of y divisible by d.

For example, the solution $(9;4,2,1)$ gives rise to $(3;4,3,2)$, and the soution to $(2;5,4,3)$ gives rise to $(4;5,3,2)$.

4. If $d = rs^3$, then $g_d(x,y,z) = g_s(x,ry,r^2z)$, so that we can obtain solutions for $d = rs^3$ if we can find solutions for $d = s$ that with the second and third variables divisible by r and r^2 respectively.

5. When $d = s^3 + 2s$, then $g_d(2,3s,-3) = 8$. Hence

$$g_d((2,3s,-3) * (2,3s,-s)) = g_d(4 - 18sd, 12s + 9d, -12 + 9s^2) = 64.$$

If $s = 2r$ is even, then each entry is the square of $(2,3s,-s)$ is even; if we divide them by 4, we get a solution of $g_d(x,y,z) = 1$. We have that

r	d	Solution	Inverse solution
r	$4r(2r^2+1)$	$(1-36r^2(2r^2+1), 3r(6r^2+5), 3(3r^2-1))$	
1	12	$(-107, 33, 6)$	(9073, 3963, 1731)
2	72	$(-1205, 174, 33)$	
3	228	$(-6155, 531, 780$	

Appendix. We have solutions for small values of d, most derived from the previous considerations.

d	positive solution	mixed solution
2	(1, 1, 1)	$(-1, 1, 0)$
	(5, 4, 3)	$(1, -2, 1)$
	(19, 15, 12)	$(1, 3, -3)$
3	(4, 3, 2)	$(-2, 0, 1)$
4	(5, 3, 2)	$(1, 1, -1)$
5	(41, 24, 14)	$(1, -4, 2)$
6	(109, 60, 33)	$(1, -6, 3)$
7	(4, 2, 1)	$(2, -1, 0)$
		$(1, -3, 3)$
9	(4, 2, 1)	$(-2, 1, 0)$
	(649, 312, 150)	$(1, 12, -6)$
10	(181, 84, 39)	$(1, 6, -3)$
11	(89, 40, 18)	$(1, 4, -2)$
12	(9073, 3963, 731)	$(-107, 33, 6)$
13	(94, 40, 17)	$(-4, -3, 2)$
14	(29, 12, 3)	$(1, 2, -1)$
15	(5401, 2190, 888)	$(1, -30, 12)$
16	(16001, 6350, 2520)	$(1, 50, -29)$
17	(314892, 122465, 47628)	$(324, -252, 49)$
18	(55, 21, 8)	$(1, -3, 1)$
19		$(-8, 3, 0)$
	(12304,4611, 1728)	$(64, -48, 9)$
20	(3191001, 144046, 53067)	$(361, -266, 49)$
21	(1705, 618, 224)	$(-47, 6, 4)$
22	(793, 283, 101)	$(23, 3, 4)$
24	(649, 225, 78)	$(1, -9, 3)$
26	(9, 3, 1)	$(3, -1, 0)$
		$(1, -27, 9)$
28	(9, 3, 1)	$(-3, 1, 0)$
		$(1, 27, -9)$
30	(811, 261, 84)	$(1, 9, -3)$
36	(109, 33, 10)	$(1, 3, -1)$
37	(100, 30, 9)	$(10, -3, 0)$
39	(529, 156, 46)	$(-23, 0, 2)$
40	(5041, 1474, 431)	$(-79, 6, 5)$
43	(49, 14, 4)	$(-7, 2, 0)$
52	(209, 56, 15)	$(1, -4, 1)$
58	(929, 240, 52)	$(1, -8, 2)$
60	(2161, 552, 141)	$(1, -12, 3)$
61	(3905, 992, 252)	$(1, -16, 4)$
62	(8929, 2256, 570)	$(1, -24, 6)$
63	(16, 4, 1)	$(4, -1, 0)$
		$(1, -48, 12)$
65	(16, 4, 1)	$(-4, 1, 0)$
		$(1, 48, -12)$
66	(9505, 2352, 582)	$(1, 24, -6)$
67	(4289, 1056, 200)	$(1, 16, -4)$
68	(2449, 600, 147)	$(1, 12, -3)$
70	(1121, 272, 66)	$(1, 8, -2)$

d	positive solution	mixed solution
72		$(-1295, 174, 35)$
76	(305, 72, 17)	$(1, 4, -1)$
86	(565, 128, 29)	$(-7, 6, 1)$
91	(18, 8, 4)	$(9, -2, 0)$
110	(551, 115, 24)	$(1, -5, 1)$
120	(5401, 1095, 222)	$(1, -15, 3)$
122	(15251, 3075, 620)	$(1, -25, 5)$
124	(25, 5, 1)	$(5, -1, 0)$
		$(1, -75, 15)$
126	(25, 5, 1)	$(-5, 1, 0)$
		$(1, 75, -15)$
128	(16001, 3175, 630)	$(1, 25, -5)$
130	(5851, 1155, 228)	$(1, 15, -3)$
140		$(1, 5, -1)$
182		$(-17, 3, 0)$
198		$(1, -6, 1)$
207		$(1, -12, 2)$
210		$(1, -18, 3)$
213		$(1, -36, 6)$
215	(36, 6, 1)	$(6, -1, 0)$
		$(1, -108, 18)$
217	(36, 6, 1)	$(-6, 1, 0)$
		$(1, 108, -18)$
219		$(1, 36, -6)$
222		$(1, 18, -3)$
228		$(-6155, 531, 78)$
225		$(1, 12, -2)$
239		$(1, 6, -1)$
240		$(1, 6, -1)$
254		$(19, -3, 0)$