RAD HAZU. MATEMATIČKE ZNANOSTI
Vol. 20 = 528 (2016): 19-26

ON CRUSSOL'S METHOD FOR $\sum_{i=1}^{4} X_i^n = \sum_{i=1}^{4} Y_i^n, n = 2, 4, 6$

Allan J. MacLeod

Abstract. Crussol gave a method for computing non-trivial integer solutions to the equations in the title. We show that the method can be linked to finding points on either of two possible elliptic curves, both of which have rank greater than zero.

1. Introduction

Towards the end of the first section in Chapter XXIV of [1], there is mention of a method to find a non-trivial solution of

$$\sum_{i=1}^{4} X_i^n = \sum_{i=1}^{4} Y_i^n \qquad n = 2, 4, 6 \tag{1.1}$$

in integers. A non-trivial solution is one where the integers X_i and Y_i are not just a permutation of each other. The method is attributed to Crussol from 1913, but with no first name or even a first initial given.

As is standard in Dickson's History, the reference to the paper just gives the journal and the date. This is the 1913 volume 8 of Sphinx-Oedipe which the present author has been unable to access.

In a survey article from 1950, Gloden [2] states that Crussol is a pseudonym for a mathematician called Roux, but, again, with no indication of a first name or letter. Gloden does state that the Crussol/Roux method is "élégante", which the method certainly is. The present work puts the method into a more general form and uses the theory of elliptic curves to allow us to derive solutions using standard software.

In the method, we take

$$X_1 = x + a, \qquad X_2 = x - a, \qquad X_3 = y + b, \qquad X_4 = y - b$$

and

$$Y_1 = z + a, \qquad Y_2 = z - a, \qquad Y_3 = t + b, \qquad Y_4 = t - b$$

2010 *Mathematics Subject Classification.* 11D09, 11Y50.
Key words and phrases. Elliptic curve, Crussol, multigrade.

and we can assume, without loss of generality, that $x, y, z, t, a, b \in \mathbb{Q}$. A purely integer result can be found by suitable scaling of a rational solution.

Substituting into (1.1) with $n = 2$, gives the equation

$$x^2 + y^2 = z^2 + t^2. \tag{1.2}$$

With $n = 4$, a non-trivial solution requires

$$x^4 + 6a^2x^2 + y^4 + 6b^2y^2 = z^4 + 6a^2z^2 + t^4 + 6b^2t^2$$

and using $t = \sqrt{x^2 + y^2 - z^2}$ this reduces to

$$4(x + z)(z - x)(y^2 - z^2 - 3(a^2 - b^2)) = 0$$

and a non-trivial solution requires, therefore,

$$y^2 - z^2 = 3(a^2 - b^2). \tag{1.3}$$

For $n = 6$ we derive a complicated expression, where we use the t formula above and $y = \sqrt{z^2 + 3a^2 - 3b^2}$ to reduce the equation to

$$x^2 + z^2 = 2a^2 + 8b^2. \tag{1.4}$$

Thus, to use Crussol's method we have to consider 3 quadrics in $\mathbb{P}^5$.

2. Crussol's Method

Dickson gives a description of Crussol's method which we summarize in this section. Crussol considers the equation (1.2) and combines (1.3) and (1.4) into the equivalent

$$y^2 + t^2 - x^2 - z^2 = 6(a^2 - b^2), \qquad x^2 + y^2 + z^2 + t^2 = 10(a^2 + b^2). \tag{2.1}$$

Then, he/she defines

$$x = \alpha q - \beta p, \qquad y = \alpha p + \beta q, \qquad z = \alpha q + \beta p, \qquad t = \alpha p - \beta q$$

which automatically satisfy (1.2). The equations in (2.1) become

$$3(a^2 - b^2) = (p^2 - q^2)(\alpha^2 - \beta^2), \qquad 5(a^2 + b^2) = (p^2 + q^2)(\alpha^2 + \beta^2). \tag{2.2}$$

He/she then defines

$$\alpha = 2\delta + \gamma, \qquad \beta = 2\gamma - \delta, \qquad a = \gamma p + \delta q, \qquad b = \gamma q - \delta p$$

which satisfies the right-hand equation in (2.2). We also have $\alpha^2 + \beta^2 = 5(\gamma^2 + \delta^2)$.

The left-hand equation becomes

$$\gamma^2 - \frac{2(p - 2q)(2p + q)}{3(p^2 - q^2)}\gamma\delta - \delta^2 = 0.$$

For this to give rational solutions, the discriminant must be a rational square so that

$$13p^4 - 12p^3q - 17p^2q^2 + 12pq^3 + 13q^4 = \square.$$

A simple solution is $p = 3, q = 2$, which gives $\gamma = 3, \delta = 5$. Using the various definitions and clearing common factors, we find

$$2^n + 16^n + 21^n + 25^n = 5^n + 14^n + 23^n + 24^n$$

for $n = 2, 4, 6$.

A second simple solution is $p = 1, q = 6$, giving $\gamma = 15, \delta = 7$ and

$$42^n + 47^n + 104^n + 125^n = 13^n + 70^n + 96^n + 127^n$$

for $n = 2, 4, 6$.

3. Elliptic Curve Method

(1.2) can be written

$$\begin{pmatrix} z \\ t \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{3.1}$$

and since we want $x, y, z, t \in \mathbb{Q}$, we must have $\cos\theta$ and $\sin\theta$ also rational.

Thus,

$$\cos\theta = \frac{1 - j^2}{1 + j^2}, \qquad \sin\theta = \frac{2j}{1 + j^2} \tag{3.2}$$

with $j \in \mathbb{Q}$.

(1.3) can be written

$$\begin{pmatrix} z \\ \sqrt{3}a \end{pmatrix} = \begin{pmatrix} \cos\mu & -\sin\mu \\ \sin\mu & \cos\mu \end{pmatrix} \begin{pmatrix} y \\ \sqrt{3}b \end{pmatrix} \tag{3.3}$$

so that

$$z = y\cos\mu - b(\sqrt{3}\cos\mu), \qquad 3a = y(\sqrt{3}\sin\mu) + 3b\cos\mu \tag{3.4}$$

Since $a, b, y, z \in \mathbb{Q}$, we must have $\cos\mu$ and $\sqrt{3}\sin\mu$ rational. Let $\cos\mu = F/H$ and $\sqrt{3}\sin\mu = G/H$, with $F, G, H \in \mathbb{Z}$, so that

$$3F^2 + G^2 = 3H^2.$$

Using the standard method of parameterizing a quadric, we have

$$\cos\mu = \frac{3k^2 - 1}{3k^2 + 1}, \qquad \sqrt{3}\sin\mu = \frac{6k}{3k^2 + 1} \tag{3.5}$$

with $k \in \mathbb{Q}$.

Thus

$$y = \frac{a(3k^2 + 1) + b(1 - 3k^2)}{2k}, \qquad z = \frac{a(3k^2 - 1) - b(3k^2 + 1)}{2k}. \tag{3.6}$$

Now, $z = ((1-j^2)x - 2jy)/(1+j^2)$, and substituting these two formulae for y and z, we have a slightly more complicated formula for x in terms of a, b, j, k,

(3.7)
$$x = \frac{a((j^2+1)(3k^2-1) + 2j(3k^2+1)) - b((j^2+1)(3k^2+1) + 2j(3k^2-1))}{2k(1-j^2)}.$$

Substituting into (1.4) gives the quadratic equation in a and b

$$a^2 - \frac{f_1(j,k)}{f_2(j,k)}ab + b^2 = 0 \tag{3.8}$$

where

$$f_1 = 2(j^2+1)(j(3k^2+1) + 3k^2 - 1)(j(3k^2-1) + 3k^2 + 1)$$

and

$$f_2 = j^4(9k^4 - 10k^2 + 1) + 2j^3(3k^2+1)(3k^2-1) + 2j^2(9k^4 + 10k^2 + 1) + 2j(3k^2+1)(3k^2-1) + 9k^4 - 10k^2 + 1.$$

The equation (3.8) has rational solutions for a, b if $f_1^2 - 4f_2^2$ is a rational square. After removing square factors, we must have $D \in \mathbb{Q}$ such that

$$D^2 = (9k^2(j^2+1) - 5(j-1)^2)(5k^2(j+1)^2 - j^2 - 1) \tag{3.9}$$

or, written alternatively as

$$D^2 = (j^2(5k^2-1) + 10jk^2 + 5k^2 - 1)(j^2(9k^2-5) + 10j + 9k^2 - 5). \tag{3.10}$$

The quartic (3.9) is made square with $k = 1$, whilst (3.10) is a square when $j = 2$. Thus both quartics are birationally equivalent to elliptic curves. Using standard methods described by Mordell in [3], we find that (3.9) is equivalent to the curve

$$E_j : \quad V^2 = U(U + (j^2-4)^2)(U + (4j^2-1)^2) \tag{3.11}$$

defined over $\mathbb{Q}(j)$, with $k = 1 + 1/f$ where

$$f = \frac{V - (7j^2+5j+7)U + (j^2-4)^2(4j^2-1)^2}{2(j+2)(2j+1)(U - (j-2)^2(2j-1)^2)}. \tag{3.12}$$

The quartic (3.10) is equivalent to

$$E_k : \quad V^2 = U^3 - 4(45k^4 - 59k^2 + 5)U^2 + 100(k^2-1)^2(9k^2-1)^2U \tag{3.13}$$

defined over $\mathbb{Q}(k)$, with $j = 2 + 1/g$ and

$$g = \frac{V + (7-33k^2)U + 60(k^2-1)^2(9k^2-1)}{10(9k^2-1)(U - 9(k^2-1)^2)}. \tag{3.14}$$

4. Elliptic Curve Properties

The curves E_j have discriminant

$$\Delta = 3600(j+1)^2(j-1)^2(j+2)^4(j-2)^4(j^2+1)^2(2j+1)^4(2j-1)^4$$

so we must assume $|j| \neq 1, 2, 1/2$ for a non-singular curve.

The curves have 3 points of order two at $(-(j^2-4)^2, 0)$, $(-(4j^2-1)^2, 0)$ and $(0,0)$. Investigation finds points of order 4 at

$$(\,(j^2-4)(4j^2-1)\,,\,\pm\,5(j^2-1)(j^2-4,(4j^2-1)\,)$$

and

$$(\,-(j^2-4)(4j^2-1)\,,\,\pm\,3(j^2-4)(4j^2-1)(j^2+1)\,)$$

and we now show that the torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

The presence of 3 points of order two and 4 points of order 4 means that the only alternative torsion structure is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Suppose P is a point of order 8, $2P$ must have order 4, and the form of the elliptic curve gives that the U-coordinate of $2P$ must be a rational square.

Consider first $d^2 = (j^2-4)(4j^2-1) = 4j^4 - 17j^2 + 4$. This is birationally equivalent to the elliptic curve $G^2 = H^3 + 136H^2 + 3600H$ with $j = 8H/G$. This curve has rank 0 using `ellrank`. Thus the only rational points are the torsion points $(0,0)$, $(-36,0)$, $(-100,0)$, $(60, \pm 960)$ and $(-60, \pm 240)$. These points only give $j = \pm 2, \pm 1/2$, which have already been excluded as giving singular curves.

For $d^2 = -(j^2-4)(4j^2-1) = -4j^4 + 17j^2 - 4$, $j = 1$ gives $d = 3$, so the quartic is birationally equivalent to the elliptic curve $G^2 = H(H+144)(H+225)$ with $j = (9H+G)/(G-9H)$. This curve also has rank 0, and 7 finite torsion points $(0,0)$, $(-144,0)$, $(-225,0)$, $(180, \pm 4860)$ and $(-180, \pm 540)$. These points all lead to values of j which give a singular elliptic curve.

Thus all non-singular curves have $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ torsion.

The denominator of (3.12) is zero when $U = (j-2)^2(2j-1)^2$ which gives $V = \pm 5(j-2)^2(j^2+1)(2j-1)^2$. Comparing this with the above torsion points, we only have equality when $|j| = 0, 1, 2, 1/2$, so, for all other values of j this must be a point of infinite order. Numerical tests suggest that the rank is often exactly 1 so no other general points of infinite order are possible.

For the curves E_k, the discriminant is

$$\Delta = 2^{12}3^2 5^4 k^2(k+1)^4(k-1)^4(3k+1)^4(3k-1)^4(10-9k^2)(10k^2-1)$$

so we have a singular curve when $|k| \neq 0, 1, 1/3$.

The cubic part of E_k has 3 rational roots only for the rational value $k = 0$, which gives a singular curve. So, non-singular curves only have one point of order 2, namely $(0,0)$. It is straightforward to show that there are two points of order 4, at $(\,10(k^2-1)(9k^2-1), \pm 60k(k^2-1)(9k^2-1)\,)$.

The transformation (3.14) has a zero denominator when $U = 9(k^2-1)^2$ which gives $V = \pm 3(k^2-1)^2(81k^2+1)$.

5. Solutions

We can derive parametric solutions from both the E_j and E_k curves by using the formulae for points of infinite order. For example, for E_j with point $((j+2)^2(2j+1)^2, -5(j+2)^2(j^2+1)(2j+1)^2)$, we just follow through all the various formulae and eventually arrive at Table 1.

Table 1. Parametric solution for X_i, Y_i

i	X_i	Y_i
1	$4j^5-4j^4-13j^3+15j^2+4j+4$	$4j^5-8j^4-13j^3-32j^2+4j$
2	$4j^5+8j^4-13j^3+32j^2+4j$	$4j^5+4j^4-13j^3-15j^2+4j-4$
3	$4j^4-32j^3-13j^2-8j+4$	$4j^5+4j^4+15j^3-13j^2-4j+4$
4	$4j^5-4j^4+15j^3+13j^2-4j-4$	$4j^4+32j^3-13j^2+8j+4$

Similarly, for the E_k curves we find the solutions in Table 2.

Table 2. Another parametric solution for X_i, Y_i

i	X_i
1	$9477k^5+30051k^4+8190k^3+1938k^2-1027k+11$
2	$13122k^5-12636k^4-11844k^3-4056k^2+2k+52$
3	$25515k^5+243k^4+162k^3-7950k^2-77k+27$
4	$2916k^5-42930k^4+3816k^3+1956k^2+948k+14$

i	Y_i
1	$25515k^5-243k^4+162k^3+7950k^2-77k-27$
2	$2916k^5+42930k^4+3816k^3-1956k^2+948k-14$
3	$9477k^5-30051k^4+8190k^3-1938k^2-1027k-11$
4	$13122k^5+12636k^4-11844k^3+4056k^2+2k-52$

Parametric solutions, however, miss out all the points on E_j and E_k which do not come from an algebraic form. Analysis of sample curves with Denis Simon's excellent `ellrank` software package [5] shows curves can have ranks of the order $3-5$ reasonably often, and higher ranks on rare occasions. We use the software package `Pari-gp` for all computations.

We wrote a `Pari` program which took a rational value of j or k, and used `ellrank` to find the rank and generators of E_j or E_k. Using these generators $G_1, \ldots, G_r$ and the torsion points, we formed points P on the curves with

$$P = n_1 G_1 + n_2 G_2 + \ldots + n_r G_r + T$$

where $|n_i| \leq L$, for some small integer limit L, and T is a torsion point.

From this we computed x, y, z, t, a, b and the solutions X_i and Y_i. Simple permutation solutions were rejected.

A huge number of different solutions can be generated very quickly. Table 3 gives solutions with one of the integers in the range $1 - 9$. As yet, we have not found a primitive solution starting with an 8.

TABLE 3. Numerical solutions

X_i	Y_i
(1, 400, 421, 882)	(216, 245, 482, 881)
(2, 16, 21, 25)	(5, 14, 23, 24)
(3, 2693, 2986, 3620)	(492, 2411, 3338, 3475)
(4, 195, 223, 271)	(41, 173, 249, 260)
(5, 29299, 32031, 37124)	(3455, 27396, 35221, 35491)
(6, 4153, 4355, 7864)	(1079, 3504, 4790, 7853)
(7, 369, 394, 635)	(191, 229, 457, 630)
(9, 389, 448, 562)	(103, 331, 504, 542)

ACKNOWLEDGEMENTS.

The author would like to express his sincere thanks to the referee for several helpful comments on the original submission.

REFERENCES

[1] L. E. Dickson, History of the Theory of Numbers, Volume II: Diophantine Analysis, AMS Publishing, New York, 1992.

[2] A. Gloden, *Aperçu historique des multigrades*, Bull. Soc. Nat. Luxemb. **54** (1950) 5–17.

[3] L.J. Mordell, Diophantine Equations, Academic Press, London, 1969.

[4] J. H. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, New York, 1992.

[5] D. Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. **5** (2002) 7–17.

O Crussolovoj metodi za $\sum_{i=1}^{4} X_i^n = \sum_{i=1}^{4} Y_i^n, n = 2, 4, 6$

Allan J. MacLeod

Sažetak. Crussol je dao metodu za računanje netrivijalnih cjelobrojnih rješenja jednadžbe iz naslova. Pokazujemo da se ta metoda može povezati s nalaženjem točaka na dvjema eliptičkim krivuljama, koje obje imaju pozitivan rang.

Statistics, O.R. and Mathematics Group (retired),
University of the West of Scotland,
High St., Paisley,
Scotland. PA1 2BE, UK

E-mail: peediejenn@hotmail.com

Received: 27.8.2015.
Revised: 10.5.2016.