An observation on Rolle's problem

Ralph H. Buchholz

In an earlier edition of the *Gazette* [3], Michael Hirschhorn considers the problem of finding three distinct integers a, b, c such that $a \pm b$, $a \pm c$, $b \pm c$ are all squares. In 1682 Rolle [2] had already provided a two parameter family of such 3-tuples,

$$\begin{aligned}
a &= y^{20} + 21y^{16}z^4 - 6y^{12}z^8 - 6y^8z^{12} + 21y^4z^{16} + z^{20},\\
b &= 10y^2z^{18} - 24y^6z^{14} + 60y^{10}z^{10} - 24y^{14}z^6 + 10y^{18}z^2,\\
c &= 6y^2z^{18} + 24y^6z^{14} - 92y^{10}z^{10} + 24y^{14}z^6 + 6y^{18}z^2,
\end{aligned}$$

however they did not provide all such solutions.

Hirschhorn sets these 6 squares to m^2, n^2, p^2, q^2, r^2, s^2 respectively and then goes on to show that this problem is equivalent to finding rational values k, l, Y such that

$$k(k^2-1)(l^4-1) = Y^2 \tag{1}$$

where $k = (m+p)/(q-n) = (q+n)(m-p)$ and $l = (p+q)(r-s) = (r+s)(p-q)$. Hirschhorn completely solves the case of $k = l^2$.

When I first read the article and saw equation (1) I immediately thought of a parameterised elliptic curve (see [5]). As a result, the machinery developed there can be applied here. Set $l = u/v$ in equation (1) and then multiply by $v^4(u^4-v^4)^2$ to obtain $[v^2(u^4-v^4)Y]^2 = (u^4-v^4)^3k^3 - (u^4-v^4)^3k$. Now transform this by letting $x := (u^4-v^4)k$ and $y := v^2(u^4-v^4)Y$ to get

$$E[u,v]:\ y^2 = x^3 - (u^4-v^4)^2x, \tag{2}$$

which is a two parameter elliptic curve equivalent to (1). Notice that (2) is symmetric in u, v so it is sufficient to consider the region $u > v \geq 1$. Furthermore, if (u^4-v^4) is divisible by a square, σ say, then we can transform $E[u,v]$, via $(x,y) \mapsto (\sigma^2x, \sigma^3y)$, to a curve of the same form with a smaller x coordinate. Hence we need only consider coprime pairs (u,v) with distinct squarefree (u^4-v^4) parts. Each particular choice of u and v corresponds to a specific elliptic curve and we show the rank of the first few in Table 1 (obtained using the techniques of [1] as implemented in `apecs`, a Maple package by Ian Connell). Note that each of these examples has rank ≥ 1 and so generates infinitely many solutions. For example we consider the curve $E[7,1]$ or $y^2 = x^3 - 2400^2x$. Then map $(x,y) \mapsto (20^2\overline{x}, 20^3\overline{y})$ to obtain $\overline{y}^2 = \overline{x}^3 - 36\overline{x}$. The point $(\overline{x},\overline{y}) = (12,36)$ is a generator of the torsion-free part of the group of rational points on this latter curve. Thus we get $k = 20^2 \cdot 12/2400 = 2$ and substituting $(k,l) = (2,7)$ into Hirschhorn's quadratic defining p/q in terms of k, l, namely

$$\begin{aligned}
&\{(k^2+1)^2(l^4+1) - 2(k^4-6k^2+1)l^2\}(p/q)^2\\
&\qquad - 2\{(k^2+1)^2(l^4-1) + 8k(k^2-1)l^2\}(p/q)\\
&\qquad\qquad + \{(k^2+1)^2(l^4+1) + 2(k^4-6k^2+1)l^2\} = 0,
\end{aligned}$$

u	v	$(u^4 - v^4)^2$	sqf $(u^4 - v^4)$	rank $(E[u,v](\mathbb{Q}))$
2	1	15^2	15	1
3	1	80^2	5	1
3	2	65^2	65	2
4	1	255^2	255	1
4	3	175^2	7	1
5	1	624^2	39	1
5	2	609^2	609	2
5	3	544^2	34	2
5	4	369^2	41	2
6	1	1295^2	1295	1
6	5	671^2	671	1
7	1	2400^2	6	1

Table 1. Rank of the first few curves $E[u,v](\mathbb{Q})$

gives the solutions $p/q = 3/4$ or $4947/3796$. By using the defining equations for k and l one finds that the first is degenerate while the second leads to the solution

$$(m,n,p,q,r,s) = (12010, 3360, 2\cdot 4947, 2\cdot 3796, 9306, 6808),$$
$$(a,b,c) = (77764850, 66475250, 20126386).$$

All multiples of $(12,36)$ in the group $E[7,1](\mathbb{Q})$ lead to solutions in the same way.

In the reverse direction it is known, from work on the congruent number problem [4], that the curves

$$E[n]:\ y^2 = x^3 - n^2x$$

for $n = 1,2,3,4,8,9,10,11,12$ (as well as infinitely many others) have zero rank and hence only finitely many rational points (in fact, just $(0,0)$, $(\pm n, 0)$ and the point at infinity). For example, Fermat had already shown (by infinite descent) that the equation $u^4 - v^4 = w^2$ is impossible in non-trivial integers. Thus we conclude that the curves $E[u,v]$ which correspond (via the mapping above with $\sigma = w$) to $E[n]$ for the values $n = 1,4,9$ have only trivial solutions. Notice that none of the rank zero n values appear in the sqf $(u^4 - v^4)$ column of Table 1 while the missing values $n = 5,6,7$ do appear.

Finally, I ran a short search covering the region $1 \le m,n,p,q,r,s \le 1850$ to confirm Hirschhorn's suspicion that Euler had in fact found the smallest possible solution, namely the first row in the following table.

a	b	c
434657	420968	150568
733025	488000	418304
993250	949986	856350
1738628	1683872	602272

Table 2. Smallest four solutions to Rolle's problem

Acknowledgment The author would like to thank the anonymous referee for pointing out the reference to Rolle's contribution.

References

[1] B.J. Birch and H.F.P. Swinnerton-Dyer, *Notes on Elliptic Curves II*, J. Reine Angew. Math. **218** (1965), 79–108.

[2] L.E. Dickson, *History of the Theory of Numbers*, vol. II (Chelsea Publishing Company New York 1952), 447.

[3] M. Hirschhorn, *A Diophantine Equation*, AustMS Gazette **20** (1993), 1–3.

[4] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms* (Springer-Verlag New York 1993).

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

E-mail: teufel_pi@yahoo.com

Received 16 May 2005, accepted 23 May 2005.