Electronic Journal: Southwest Journal of Pure and Applied Mathematics
Internet: http://rattler.cameron.edu/swjpam.html
ISSN 1083-0464
Issue 2, December 2003, pp. 9–17.
Submitted: October 13, 2003. Published: December 31 2003.

A SOLUTION TO AN "UNSOLVED PROBLEM IN NUMBER THEORY"

Allan J. MacLeod

Abstract. We discuss the problem of finding integer-sided triangles with the ratio base/altitude or altitude/base an integer. This problem is mentioned in Richard Guy's book "Unsolved Problems in Number Theory". The problem is shown to be equivalent to finding rational points on a family of elliptic curves. Various computational resources are used to find those integers in $[1, 99]$ which do appear, and also find the sides of example triangles.

A.M.S. (MOS) Subject Classification Codes. 11D25 , 11Y50

Key Words and Phrases. Triangle, Elliptic curve, Rank, Descent

1. Introduction

Richard Guy's book Unsolved Problems in Number Theory [5] is a rich source of fascinating problems. The final 3 paragraphs in section D19 of this book discuss the following problem:

Problem Which integers N occur as the ratios base/height in integer-sided triangles?

Also mentioned is the dual problem where height/base is integer. Some numerical examples are given together with some more analytical results, but no detailed analysis is presented.

Let BCD be a triangle with sides b,c,d using the standard naming convention. Let a be the height of B above the side CD. If one of the angles at C or D is obtuse then the height lies outside the triangle, otherwise it lies inside.

Assume, first, that we have the latter. Let E be the intersection of the height and CD, with $DE = z$ and $EC = b - z$. Then

Department of Mathematics and Statistics, University of Paisley,
High St., Paisley, Scotland. PA1 2BE
E-mail Address:allan.macleod@paisley.ac.uk

$$(1)\qquad \begin{aligned} a^2 + z^2 &= c^2 \\ a^2 + (b-z)^2 &= d^2 \end{aligned}$$

Now, if base/height = N, the second equation is

$$a^2 + (z - Na)^2 = d^2$$

For altitudes outside the triangle the equations are the same, except for $z - Na$ replaced by $z + Na$. We thus consider the general system, with N positive or negative.

$$(2)\qquad \begin{aligned} a^2 + z^2 &= c^2 \\ a^2 + (z-Na)^2 &= d^2 \end{aligned}$$

Clearly, we can assume that a and z have no common factors, so there exists integers p and q (of opposite parities) such that (1) $a = 2pq$,$z = p^2 - q^2$, or (2) $a = p^2 - q^2$, $z = 2pq$.

As a first stage, we can set up an easy search procedure. For a given pair (p, q), compute a and x using both the above possibilities. For N in a specified range test whether the resulting d value is an integer square.

This can be very simply done using the software package UBASIC, leading to the results in Table 1, which come from searching with $3 \leq p + q \leq 999$ and $-99 \leq N \leq 99$.

This table includes results for the formulae quoted in Guy, namely $N = 2m(2m^2+1)$ and $N = 8t^2 \pm 4t + 2$, and the individual values quoted except for $N = 19$. It also includes solutions from other values.

It is possible to extend the search but this will take considerably more time and there is no guarantee that we will find all possible values of N. We need alternative means of answering the following questions:

(1) can we say for a specified value of N whether a solution exists?

(2) if one exists, can we find it?

2. Elliptic Curve Formulation

In this section, we show that the problem can be considered in terms of elliptic curves.

Assuming $a = 2pq$ and $z = p^2 - q^2$, then the equation for d is

$$(3)\qquad d^2 = p^4 - 4Np^3q + (4N^2 + 2)p^2q^2 + 4Npq^3 + q^4$$

Define $j = d/q^2$ and $h = p/q$, so that

TABLE 1. Solutions for $2 \leq N \leq 99$

N	b	c	d	N	b	c	d
5	600	241	409	6	120	29	101
8	120	17	113	9	9360	1769	10841
13	291720	31849	315121	14	2184	685	1525
15	10920	2753	8297	18	6254640	439289	6532649
20	46800	8269	54781	26	15600	5641	10009
29	3480	169	3601	29	737760	31681	719329
29	706440	336841	371281	34	118320	4441	121129
36	4896	305	4625	40	24480	1237	23413
40	24360	3809	20609	40	741000	274853	1015397
42	24360	3389	21029	42	68880	26921	42041
42	2270520	262909	2528389	48	118320	4033	121537
61	133224	2305	132505	62	226920	93061	133981
68	4226880	90721	4293409	86	614040	260149	354061
94	3513720	42709	3493261	99	704880	198089	506969

$$j^2 = h^4 - 4Nh^3 + (4N^2 + 2)h^2 + 4Nh + 1 \tag{4}$$

This has an obvious rational point $h = 0, j = 1$, and so is birationally equivalent to an elliptic curve, see Mordell [7]. Using standard algebra, we can can link this equation to the curve

$$E_N : y^2 = x^3 + (N^2 + 2)x^2 + x \tag{5}$$

with the transformations $h = p/q = (Nx + y)/(x + 1)$.

If, however, $a = p^2 - q^2$ and $z = 2pq$, we have a different quartic for d^2, but leading to the same elliptic curve, with the relevant transformation $p/q = (Nx + x + y + 1)/(Nx - x + y - 1)$.

Thus the existence of solutions to the original problem is related to the rational points lying on the curve. There is the obvious point $(x, y) = (0, 0)$, which gives $p/q = 0$ or $p/q = -1$, neither of which give non-trivial solutions. A little thought shows the points $(-1, \pm N)$, giving $p/q = \infty$, $p/q = 0/0$, or $p/q = 1$, again failing to give non-trivial solutions.

We can, in fact, invert this argument and show the following

Lemma: If (x, y) is a rational point on the elliptic curve E_N with $x \neq 0$ or $x \neq -1$, then we get a non-trivial solution to the problem.

The proof of this is a straightforward consideration of the situations leading to $p^2 - q^2 = 0$ or $pq = 0$, and showing that the only rational points which can cause these are $x = 0$ or $x = -1$. It is also clear that if a or z become negative we can essentially ignore the negative sign.

3. Torsion Points

It is well known that the rational points on an elliptic curve form a finitely-generated group, which is isomorphic to the group $T \oplus \mathbb{Z}^r$, where $r \geq 0$ is the rank of the elliptic curve, and T is the torsion subgroup of points of finite order.

We first consider the torsion points. The point at infinity is considered the identity of the group. Points of order 2 have $y = 0$, so $(0, 0)$ is one. The other roots of $y = 0$ are irrational for N integral, so there is only one point of order 2. Thus, by Mazur's theorem, the torsion subgroup is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, with the symmetry of the curve about $y = 0$ ensuring N one of $2, 4, 6, 8, 10, 12$.

For elliptic curves of the form $y^2 = x(x^2 + ax + b)$, a point $P = (x, y)$ leads to 2P having x-coordinate $(x^2 - b)^2/4y^2$. Thus, if P has order 4, then 2P has order 2, so 2P=(0,0) for the curves E_N. Thus $x^2 - 1 = 0$, so that $x = \pm 1$. The value $x = 1$ gives $y = \sqrt{N^2 + 4}$, which is irrational. $x = -1$ gives $y = \pm N$, so that $(-1, \pm N)$ are the only order 4 points. This reduces the possibilities for the torsion subgroup to $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, or $\mathbb{Z}/12\mathbb{Z}$.

For $\mathbb{Z}/8\mathbb{Z}$, we would have 4 points of order 8. Suppose Q is of order 8, giving 2Q of order 4. Thus the x-coordinate of 2Q must be -1, but as we stated previously, the x-coordinate of 2Q is a square. Thus there cannot be any points of order 8.

For $\mathbb{Z}/12\mathbb{Z}$, we would have 2 points of order 3, which correspond to any rational points of inflection of the elliptic curve. These are solutions to

$$3x^4 + 4(N^2 + 2)x^3 + 6x^2 - 1 = 0 \tag{6}$$

If $x = r/s$ is a rational solution to this, then $s|3$ and $r|1$, so the only possible rational roots are ± 1 and $\pm 1/3$. Testing each shows that they are not roots for any value of N.

Thus, the torsion subgroup consists of the point at infinity, (0,0), $(-1, \pm N)$. As we saw, in the previous section, these points all lead to trivial solutions. We thus have proven the following

Theorem: A non-trivial solution exists iff the rank of E_N is at least 1. If the rank is zero then no solution exists.

4. Parametric Solutions

As mentioned in the introduction, Guy quotes the fact that solutions exist for $N = 2m(2m^2 + 1)$ and $N = 8t^2 \pm 4t + 2$, though without any indication of how these forms were discovered. We show, in this section, how to use the elliptic curves E_N to determine new parametric solutions.

The simple approach used is based on the fact that rational points on elliptic curves of the form

$$y^2 = x^3 + ax^2 + bx$$

have $x = du^2/v^2$ with $d|b$. Thus, for E_N, we can only have $d = \pm 1$.

We look for integer points so $v = 1$, and searched over $1 \leq N \leq 999$ and $1 \leq u \leq 99999$ to find points on the curve. The data output is then analysed to search for patterns leading to parametric solutions.

For example, the above sequences have points P given by

1. $N = 2m(2m^2 + 1)$, $P = (4m^2, 2m(8m^4 + 4m^2 + 1))$,
2. $N = 8t^2 + 4t + 2$, $P = (-(8t^2 + 4t + 1)^2, 2(4t + 1)(4t^2 + 2t + 1)(8t^2 + 4t + 1))$,
3. $N = 8t^2 - 4t + 2$, $P = (-(8t^2 - 4t + 1)^2, 2(4t - 1)(4t^2 - 2t + 1)(8t^2 - 4t + 1))$.

These parametric solutions are reasonably easy to see in the output data. Slightly more difficult to find is the solution with $N = 4(s^2+2s+2)$, $x = (2s^3+6s^2+7s+3)^2$ and $y = (s + 1)(s^2 + 2s + 2)(2s^2 + 4s + 3)(4s^4 + 16s^3 + 32s^2 + 32s + 13)$.

Using $p/q = (Nx + y)/(x + 1)$ with $a = 2pq, z = p^2 - q^2$, we find the following formulae for the sides of the triangles:

$$b = 8(s + 1)(s^2 + 2s + 2)(2s^2 + 2s + 1)(2s^2 + 4s + 3)(2s^2 + 6s + 5)$$

$$\begin{aligned} c =& 16s^{10} + 192s^9 + 1056s^8 + 3504s^7 + 7768s^6 + 12024s^5 \\ &+ 13168s^4 + 10076s^3 + 5157s^2 + 1594s + 226 \end{aligned}$$

$$\begin{aligned} d =& 16s^{10} + 128s^9 + 480s^8 + 1104s^7 + 1720s^6 \\ &+ 1896s^5 + 1504s^4 + 868s^3 + 381s^2 + 138s + 34 \end{aligned}$$

Other parametric solutions can be found by adding the points on the curve to the torsion points.

5. Rank Calculations

We now describe a computational approach to the determination of the rank. This follows the approach of Zagier & Kramarcz [10] or Bremner & Jones [2] for example. The computations are based on the Birch and Swinnerton-Dyer (BSD) conjecture, which states (roughly) - if an elliptic curve has rank r, then the L-series of the curve has a zero of order r at the point 1. Smart [9] calls this the "conditional algorithm" for the rank.

The L-series of an elliptic curve can be defined formally as

$$L(s) = \sum_{k=1}^{\infty} \frac{a_k}{k^s}$$

where a_k are integers which depend on the algebraic properties of the curve. This form is useless for effective computation at $s = 1$, so we use the following form from Proposition 7.5.8. of Cohen [3]

$$L(1) = \sum_{k=1}^{\infty} \frac{a_k}{k} \left(\exp(-2\pi k A/\sqrt{N^*}) + \epsilon \exp(-2\pi k/(A\sqrt{N^*})) \right)$$

with $\epsilon = \pm 1$ - the sign of the functional equation, N^* - the conductor of the equation, and A **ANY** number.

N^* can be computed by Tate's algorithm - see Algorithm 7.5.3 of Cohen, while ϵ can be computed by computing the right-hand sum at two close values of A - say

1 and 1.1 - and seeing which choice of ϵ leads to agreement (within rounding and truncation error). If $\epsilon = 1$ then the curve has even rank, whilst if $\epsilon = -1$ the curve has odd rank.

We thus determine the value of ϵ. If $\epsilon = 1$, we compute

$$L(1) = 2\sum_{k=1}^{\infty} \frac{a_k}{k} \exp(-2\pi k/\sqrt{N^*})$$

and, if this is non-zero, then we assume $r = 0$, whilst, if zero, $r \geq 2$. For $\epsilon = -1$, we compute

$$L'(1) = 2\sum_{k=1}^{\infty} \frac{a_k}{k} E_1(2\pi k/\sqrt{N^*})$$

with E_1 the standard exponential integral special function. If this is non-zero, then we assume $r = 1$, whilst if zero, $r \geq 3$.

The most time-consuming aspect of these computations is the determination of the a_k values. Cohen gives a very simple algorithm which is easy to code, but takes a long time for k large. To achieve convergence in the above sums we clearly need $k = O(\sqrt{N^*})$. Even in the simple range we consider, N^* can be several million, so we might have to compute many thousands of a_k values.

6. Numerical Results

Using all the ideas of the previous section, we wrote a UBASIC program to estimate the rank of E_N for $1 \leq N \leq 99$. The results are given in the following table. We have no proof that these values are correct, but for every value of N with rank greater than 0 we have found a non-trivial solution to the original triangle problem.

TABLE 2. Rank of E_N for $1 \leq N \leq 99$

	0	1	2	3	4	5	6	7	8	9
00+		0	0	0	0	1	1	0	1	1
10+	0	0	0	1	1	1	0	1	1	1
20+	1	1	1	1	0	0	1	0	0	2
30+	0	1	1	0	1	1	1	1	1	0
40+	2	0	2	1	1	1	0	0	1	0
50+	0	0	1	2	0	0	0	0	0	0
60+	0	2	2	1	0	0	0	0	2	1
70+	0	1	1	1	1	0	1	1	0	1
80+	0	0	0	1	1	2	2	1	0	0
90+	0	0	1	1	1	1	0	1	1	2

To find an actual solution, we can assume that $x = du^2/v^2$ and $y = duw/v^3$, with $(u, v) = 1$ and d squarefree, and hence that

$$w^2 = du^4 + (N^2 + 2)u^2v^2 + v^4/d$$

implying that $d = \pm 1$.

For curves with rank 2, we found that a simple search quickly finds a solution. This also holds for a few rank 1 curves, but most curves did not produce an answer in a reasonable time.

A by-product of the L-series calculation is an estimate H of the height of a rational point on the curve. The height gives a rough idea of how many decimal digits will be involved in a point, and thus how difficult it will be to compute it. The following formula gives the height, see Silverman [8] for a more precise definition of the quantities involved.

$$H = \frac{L'(1)\, T^2}{2\, |\text{Ш}|\, \Omega\, c}$$

where T is the order of the torsion subgroup, Ш is the Tate-Safarevic group, Ω is the real period of the curve, and c is the Tamagawa number of the curve.

There is no known algorithm to determine $|\text{Ш}|$ and so we usually use the value 1 in the formula. Note that for this problem $T = 4$, and that this formula gives a value half that of an alternative height normalisation used in Cremona [4].

Unfortunately, this value is not always the height of the generator of the infinite subgroup, but sometimes of a multiple. An example comes from $N = 94$, where the height calculation gave a value $H = 55.1$, suggesting a point with tens of digits in the numerator and denominator. We actually found a point with $x = 4/441$.

To determine the values of (d, u, v, w), we used a standard descent procedure as described by Cremona or Bremner et al [1]. We consider equation (11) firstly as

$$w^2 = dz^2 + (N^2 + 2)zt + t^2/d$$

Since this is a quadratic, if we find a simple numerical solution, we can parameterise $z = f_1(r, s)$ and $t = f_2(r, s)$, with f_1 and f_2 homogeneous quadratics in r and s. We then look for solutions to $z = ku^2$, $t = kv^2$, with k squarefree.

Considering $q = kv^2$, if we find a simple numerical solution we can parameterise again for r and s as quadratics, which are substituted into $p = ku^2$, giving a quartic which needs to be square. We search this quartic to find a solution.

We wrote a UBASIC code which performs the entire process very efficiently. This enabled most solutions with heights up to about 16 to be found.

For larger heights we can sometimes use the fact that the curve E_N is 2-isogenous to the curve

$$f^2 = g^3 - 2(N^2 + 2)g^2 + N^2(N^2 + 4)g$$

with $x = f^2/4g^2$ and $y = f(g^2 - N^2(N^2+4))/8g^2$. This curve has the same rank as E_N and sometimes a point with estimated height half that of the equivalent point on E_N.

For points with height greater than about 20, however, we used a new descent method which involves trying to factorise the quartic which arises in the descent method discussed above. This method is described in the report [6]. This has enabled us to complete a table of solutions for all values in the range $1 < N \leq 99$.

The largest height solved is for $N = 79$ with E_{79} having equation $y^2 = x^3 + 6243x^2 + x$. The estimated height is roughly 40, but the 2-isogenous curve $f^2 = g^3 - 12486g^2 + 38975045g$ was indicated to have a point with height about 20.

We found a point with

$$g = \frac{2836\ 8499\ 3467\ 6319\ 5139\ 0020}{4689\ 8490\ 9449\ 9234\ 0041}$$

leading to a point on the original curve with

$$x = \frac{2654\ 7926\ 1289\ 1944\ 1996\ 8505\ 1867\ 1143\ 3025}{1705\ 4187\ 5947\ 7256\ 7676\ 9862\ 5643\ 5806\ 2336}$$

For interested readers, this point leads to the triangle with sides

$$\begin{aligned} b =& 146586997184778231835321971944006987 8\\ & 865747485658641082621328674163116496 0\end{aligned}$$

$$\begin{aligned} c =& 8927676534887485887603362942709577 50\\ & 7378277308118665999941086255389471249\end{aligned}$$

$$\begin{aligned} d =& 5735953691823056195537866267793192 92\\ & 6159738767971279754707312477117108209\end{aligned}$$

7. Altitude/Base

If we wish altitude/base=M, then we can use the theory of section 2, with $N = 1/M$. If we define $s = M^3y$, $t = M^2x$, we get the system of elliptic curves F_M, given by

$$s^2 = t^3 + (2M^2 + 1)t^2 + M^4t$$

These curves have clearly the same torsion structure as E_N, with the point at infinity, $(0, 0)$, and $(-M^2, \pm M^2)$ being the torsion points. We can also search for parametric solutions, and we found that $M = s(s + 2)$ has the following points:

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

If we call the first point Q, then the second point comes from $Q + (0, 0)$ and the third from $Q + (-M^2, M^2)$.

Considering Q, we find

TABLE 3. Rank of F_M for $1 \leq M \leq 99$

	0	1	2	3	4	5	6	7	8	9
00+		0	0	1	0	1	0	1	1	0
10+	1	0	0	1	0	1	0	0	1	0
20+	0	1	0	0	1	0	0	1	0	0
30+	1	0	0	0	0	1	0	1	0	1
40+	1	2	2	2	1	0	0	1	1	1
50+	0	1	1	0	0	2	0	1	1	0
60+	1	1	1	2	1	0	0	1	1	0
70+	1	1	1	1	1	0	1	1	0	0
80+	2	1	0	0	0	0	1	0	2	0
90+	0	1	0	1	0	1	0	0	0	1

$$b = 2(s+1)\,,\; c = s(2s^2+6s+5)\,,\; d = (s+2)(2s^2+2s+1)$$

which always gives an obtuse angle.

The BSD conjecture gives rank calculations listed in Table 3.

As before, we used a variety of techniques to find non-torsion points on F_M. We must say that these curves proved much more testing than E_N. Several hours computation on a 200MHz PC were needed for $M = 47$, while we have not been able to find a point for $M = 67$, which has an estimated height of 45.7, though this is the only value in $[1, 99]$ for which we do not have a rational point.

References

1. A. Bremner, R.K. Guy and R. Nowakowski, *Which integers are representable as the product of the sum of three integers with the sum of their reciprocals*, Math. Comp. **61** (1993), 117-130.
2. A. Bremner and J.W. Jones, *On the equation $x^4 + mx^2y^2 + y^4 = z^2$*, J. Number Theory **50** (1995), 286-298.
3. H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics 138, Springer-Verlag, New York, 1993.
4. J. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd. ed., Cambridge University Press, Cambridge, 1997.
5. R.K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer-Verlag, New York,, 1994.
6. A.J. MacLeod, *A simple practical higher descent for large height rational points on certain elliptic curves*, XXX Preprint Archive, NT9904172, 1999.
7. L.J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.
8. J.H. Silverman, *Computing rational points on rank 1 elliptic curves via L-series and canonical heights*, Math. Comp. **68** (1999), 835-858.
9. N.P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts 41, Cambridge University Press, Cambridge, 1998.
10. D. Zagier and G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. **52** (1987), 51-69.