Proceedings of the Edinburgh Mathematical Society (2009) **52**, 37–44 ©
DOI:10.1017/S0013091507000065 Printed in the United Kingdom

A PROBLEM OF OZANAM

ANDREW BREMNER

Department of Mathematics and Statistics, Arizona State University, Tempe, AZ 85287-1804, USA (bremner@asu.edu)

(Received 9 January 2007)

Dedicated to Professor Richard K. Guy in celebration of his entry into a tenth decade

Abstract A problem posed in the early eighteenth century asks for right-angled triangles, each of whose sides exceeds double the area by a perfect square. We summarize known results and find such triangles with the smallest possible standard generators.

Keywords: Pythagorean triangle; area; square; elliptic curve

2000 *Mathematics subject classification:* Primary 11D25
Secondary 11G05

Macleod [**3**] has drawn attention to the following problem mentioned in Dickson's *History of the theory of numbers* [**2**], on rational right triangles (evidently it was posed in obscure verse in *The ladies diary* for 1728 as Question 133, but seems to be based on a numerical example of Ozanam from 1702).

Find a right triangle each of whose sides exceeds double the area by a square.

Ozanam [**4**] gives the example of the triangle with sides

$$\left\{\frac{2\,264\,592}{20\,590\,417}, \frac{18\,325\,825}{20\,590\,417}, \frac{18\,465\,217}{20\,590\,417}\right\}, \tag{1}$$

which has the property that

$$\begin{aligned}
\text{side}(1) - 2\text{ area} &= \left(\frac{2\,264\,592}{20\,590\,417}\right)^2,\\
\text{side}(2) - 2\text{ area} &= \left(\frac{18\,325\,825}{20\,590\,417}\right)^2,\\
\text{side}(3) - 2\text{ area} &= \left(\frac{18\,403\,967}{20\,590\,417}\right)^2.
\end{aligned}$$

The Ozanam solution is the right triangle with standard generators (m, n) equal to $(4289, 264)$ and common multiple $1/20\,590\,417$.

There is further discussion in [**2**], but with various mistakes; and, as Macleod has observed, the 'new' solutions there all turn out to be equivalent to Ozanam's solution above. Macleod himself, in [**3**], computes a second solution, corresponding to that with standard generators

$$(m, n) = (5\,126\,077\,790\,593, 631\,550\,531\,572),$$

and common multiple $1/32\,352\,571\,748\,338\,801\,492\,704\,857$, so that the triangle has sides

$$\left\{\frac{25\,877\,817\,441\,281\,936\,590\,500\,465}{32\,352\,571\,748\,338\,801\,492\,704\,857}, \frac{6\,474\,754\,307\,056\,864\,902\,204\,392}{32\,352\,571\,748\,338\,801\,492\,704\,857}, \frac{26\,675\,529\,589\,139\,688\,128\,082\,833}{32\,352\,571\,748\,338\,801\,492\,704\,857}\right\}, \tag{2}$$

with

$$\begin{aligned}
\text{side}(1) - 2\text{ area} &= \left(\frac{25\,877\,817\,441\,281\,936\,590\,500\,465}{32\,352\,571\,748\,338\,801\,492\,704\,857}\right)^2,\\
\text{side}(2) - 2\text{ area} &= \left(\frac{6\,474\,754\,307\,056\,864\,902\,204\,392}{32\,352\,571\,748\,338\,801\,492\,704\,857}\right)^2,\\
\text{side}(3) - 2\text{ area} &= \left(\frac{26\,371\,755\,251\,071\,267\,154\,312\,449}{32\,352\,571\,748\,338\,801\,492\,704\,857}\right)^2.
\end{aligned}$$

We make the further observation that the following triangle also satisfies the demands of the problem

$$\left\{1, \frac{34\,440}{34\,969}, \frac{49\,081}{34\,969}\right\}, \tag{3}$$

though there is an arguable blemish in that the second side has the property of actually being equal to twice the area:

$$\begin{aligned}
\text{side}(1) - 2\text{ area} &= (\tfrac{23}{187})^2,\\
\text{side}(2) - 2\text{ area} &= 0^2,\\
\text{side}(3) - 2\text{ area} &= (\tfrac{11}{17})^2.
\end{aligned}$$

This triangle has generators (m, n) equal to $(205, 84)$ with common multiple $1/34\,969$.

We analyse the mathematics behind this problem, and suppose that the required right triangle be

$$\{k(m^2 - n^2), 2kmn, k(m^2 + n^2)\},$$

for integers $m > n$ of opposite parity, and rational k. Then the demands of the problem are that

$$\begin{aligned}
k(m^2 - n^2) - 2k^2mn(m^2 - n^2) &= \text{square},\\
2kmn - 2k^2mn(m^2 - n^2) &= \text{square},\\
k(m^2 + n^2) - 2k^2mn(m^2 - n^2) &= \text{square}.
\end{aligned}$$

https://doi.org/10.1017/S0013091507000065 Published online by Cambridge University Press

That is,

$$\left.\begin{aligned} K(m^2-n^2)-2mn(m^2-n^2) &= a^2/d^2,\\ K(2mn)-2mn(m^2-n^2) &= 4m^2n^2b^2/d^2,\\ K(m^2+n^2)-2mn(m^2-n^2) &= c^2/d^2, \end{aligned}\right\} \tag{4}$$

say, where $K = 1/k$. On eliminating K,

$$\left.\begin{aligned} 2mn(m^2-n^2)b^2+(m^2-n^2)(m^2-2mn-n^2)d^2 &= a^2,\\ 2mn(m^2+n^2)b^2+(m^2-n^2)(m-n)^2d^2 &= c^2. \end{aligned}\right\} \tag{5}$$

Regarded as lying in projective 3-space with underlying coordinates a, b, c, d, this intersection of two quadrics over the coefficient field $\boldsymbol{Q}(m/n)$ represents a curve of genus 1. The first quadric has a point at $(b,d,a) = (1,1,m^2-n^2)$, which leads to the following parametrization of its points:

$$\begin{aligned} b:d:a = 2mnS^2+2(m^2-n^2)ST+(m^2-n^2)T^2 : -2mnS^2+(m^2-n^2)T^2 :&\\ (m^2-n^2)(2mnS^2+4mnST+(m^2-n^2)T^2).& \end{aligned}$$

Accordingly, on the second quadric,

$$\begin{aligned} &4m^2n^2(m^4+4mn^3-n^4)S^4\\ &\quad+16m^2n^2(m^4-n^4)S^3T+4mn(m^2-n^2)(m^4+4m^3n-n^4)S^2T^2\\ &\quad+8mn(m^2-n^2)(m^4-n^4)ST^3+(m^2-n^2)^2(m^4+4mn^3-n^4)T^4 = \text{square}, \end{aligned} \tag{6}$$

which provides a quartic model for the curve of genus 1.

This curve of genus 1 is certainly elliptic in the case when

$$m^4+4mn^3-n^4 = \text{square}, \tag{7}$$

for then it contains rational points at $(S,T) = (1,0),(0,1)$. This condition on m, n is in turn just that $x = m/n$ gives a point on the elliptic curve

$$x^4+4x-1 = y^2,$$

which is discovered to be a curve of conductor 448 and Mordell–Weil rank 1 with generator $P(x,y) = (\frac{1}{4},\frac{1}{16})$. The torsion group is of order 2, and the point $(m/n,p)$ added to the non-zero torsion element is the point

$$\left(\frac{m+n}{m-n},\frac{2n^2p}{(m-n)^2}\right);$$

precisely one of these two points has x-coordinate in numerator and denominator of opposite parity. From the multiples of P we now recover the following pairs (m,n):

$$\begin{aligned} P:&\quad (1,4),\\ 2P:&\quad (-65,4),\\ 3P:&\quad (4289,64),\\ 4P:&\quad (287\,297,1\,114\,872),\\ 5P:&\quad (-1\,178\,432\,705,144\,916\,468),\\ 6P:&\quad (5\,126\,077\,790\,593,631\,550\,531\,572). \end{aligned}$$

https://doi.org/10.1017/S0013091507000065 Published online by Cambridge University Press

Of course, the physical constraints of the problem imply that we only obtain solution triangles in the case when $m > n$, and m and n are of opposite parity. Thus, the 'smallest' solution arising from the condition (7) occurs for $(m, n) = (4289, 264)$, and is indeed the Ozanam triangle at (1). The second smallest occurs for the multiple $6P$, and is that of Macleod at (2). It is straightforward to see from a density argument that infinitely many triangles of the required type arise in this manner.

In general, it is entirely possible that, for (m, n) not satisfying condition (7), (6) contains rational points, as indeed we have seen above for the case when $(m, n) = (205, 84)$, with $(S, T) = (187, -164)$. The corresponding triangle, with $b = 0$, is also one of an infinite family. Setting $b = 0$ at (5) demands

$$\begin{aligned} m^2 - 2mn - n^2 &= \text{square}, \\ m^2 - n^2 &= \text{square}, \end{aligned}$$

which is a model of an elliptic curve of conductor 128 and rational Mordell–Weil rank 1 with generator $(m, n) = (1, 0)$. The multiples of the generator give

$$(m, n) = (5, -4),\ (205, 84),\ (28\,249, -26\,040),\ (33\,816\,809, 5\,333\,240),\ \dots,$$

so that the second triangle that arises is from $(m, n) = (33\,816\,809, 5\,333\,240)$ with sides

$$\left\{1, \frac{360\,706\,316\,862\,320}{1\,115\,133\,122\,044\,881}, \frac{11\,72\,020\,019\,840\,081}{1\,115\,133\,122\,044\,881}\right\} \tag{8}$$

and

$$\begin{aligned} \text{side}(1) - 2\ \text{area} &= \left(\frac{27\,466\,831}{33\,393\,609}\right)^2, \\ \text{side}(2) - 2\ \text{area} &= 0^2, \\ \text{side}(3) - 2\ \text{area} &= \left(\frac{5337}{6257}\right)^2. \end{aligned}$$

The rational points are dense on the elliptic curve, and so we obtain infinitely many such triangles with $b = 0$.

It is intriguing to ask whether there are any examples which do not belong to either of the above two infinite families. Such an example would derive from rational points on (6) with the property that $m^4 + 4mn^3 - n^4$ is not square, and that $m^2 - n^2$, $m^2 - 2mn - n^2$ are not both squares. We decided to investigate the cases of underlying triangles possessing generators (m, n) in the range $m + n \leqslant 289$ (because of our example at $(m, n) = (205, 84)$), with the hope of discovering a solution triangle with 'smallest' generators (m, n), that is, minimizing $m + n$. In this range, the quartic (6) is everywhere locally solvable for precisely 200 values of m and n satisfying $m > n$, m and n of opposite parity. This list begins

$$(17, 8),\ (13, 12),\ (25, 4),\ (17, 12),\ (25, 12),\ (25, 16),\ (41, 4),\ (29, 16),\ \dots. \tag{9}$$

https://doi.org/10.1017/S0013091507000065 Published online by Cambridge University Press

For each of these pairs (m, n) one needs first to determine whether or not there is a rational point on (6), and this is an entirely non-trivial problem. Indeed, searching over the range $S + |T| \leqslant 10\,000$ produced only the points

$$(S, T) = (187, -164),\ (187, -210) \quad \text{when } (m, n) = (205, 84),$$

leading to the triangle at (3), and

$$(S, T) = (357, -52),\ (119, -2340) \quad \text{when } (m, n) = (169, 120),$$

leading to the triangle (with $k = 4489/215\,159\,344$)

$$\left\{\frac{219\,961}{744\,496}, \frac{11\,379\,615}{13\,447\,459}, \frac{192\,851\,929}{215\,159\,344}\right\} \tag{10}$$

with

$$\begin{aligned} \text{side}(1) - 2 \text{ area} &= \left(\frac{337\,211}{1\,582\,054}\right)^2, \\ \text{side}(2) - 2 \text{ area} &= \left(\frac{143\,715}{186\,124}\right)^2, \\ \text{side}(3) - 2 \text{ area} &= \left(\frac{1\,271\,861}{1\,582\,054}\right)^2. \end{aligned}$$

The Magma [**1**] computational package, which was used for all calculations in this paper, contains a routine 'FourDescent' for attempting a four-descent on quartics such as (6). For the first two pairs (m, n) at (9) this routine establishes that (6) has no rational point; it is likely that further pairs from (9) may be similarly eliminated, but random trials had the program churning without conclusion. Instead, we return to (5), and observe that a point (b, d, a, c) gives rise to a point on the elliptic curve $E_{m,n}$:

$$Y^2 = X(X + 2mn(m-n)^4(m+n)^2)(X + 2mn(m^4 - n^4)(m^2 - 2mn - n^2)) \tag{11}$$

under the mapping

$$X = \frac{4m^2n^2(m^4 - n^4)b^2}{d^2}, \qquad Y = \frac{4m^2n^2(m^4 - n^4)abc}{d}. \tag{12}$$

Thus, for a given pair (m, n) we seek a curve (11) of positive rational rank, with the necessary condition that it contains points P with the X-coordinate satisfying, from (12),

$$X \equiv (m^4 - n^4) \bmod \boldsymbol{Q}^{*2}. \tag{13}$$

For example, at $(m, n) = (17, 8)$, the first pair from (9), the rank of the curve $E_{17,8}$ is determined to be equal to 1, with possible generator

$$P(X, Y) = (-285\,930\,000, 17\,567\,539\,200\,000).$$

https://doi.org/10.1017/S0013091507000065 Published online by Cambridge University Press

The non-trivial torsion points are

$$T_0 = (0,0), \qquad T_1 = (-1\,115\,370\,000, 0), \qquad T_2 = (1\,015\,369\,200, 0),$$

and none of $P + T_i$ is rationally divisible by 2. It follows that P generates

$$E_{17,8}(\boldsymbol{Q})/2E_{17,8}(\boldsymbol{Q})$$

and, up to torsion, the X-coordinates of points in $E_{17,8}(\boldsymbol{Q})$ satisfy

$$X \equiv 1, -285\,930\,000 \bmod \boldsymbol{Q}^{*2},$$

that is, $X \equiv 1, -353 \bmod \boldsymbol{Q}^{*2}$. The torsion points have X-coordinates satisfying

$$X \equiv 1, -47 \cdot 353, -17, 17 \cdot 47 \cdot 353 \bmod \boldsymbol{Q}^{*2},$$

so finally the X-coordinates of points in $E_{17,8}(\boldsymbol{Q})$ satisfy

$$X \equiv 1, -353, -47 \cdot 353, 47, -17, 17 \cdot 353, 17 \cdot 47 \cdot 353, -17 \cdot 47 \bmod \boldsymbol{Q}^{*2}.$$

More succinctly, the multiplicative subgroup of $\boldsymbol{Q}/\boldsymbol{Q}^{*2}$ comprising X-coordinates of points in $E_{17,8}(\boldsymbol{Q})$ is generated by $\langle -17, 47, -353 \rangle$. But $m^4 - n^4 \equiv 353 \bmod \boldsymbol{Q}^{*2}$, and thus (13) cannot hold for any point on $E_{17,8}$.

In a similar vein, at $(m,n) = (13,12)$, where the rational rank is 1, a generator for $E_{13,12}(\boldsymbol{Q})/2E_{13,12}(\boldsymbol{Q})$ is

$$\left(\frac{5\,298\,333\,054\,885\,000}{3\,924\,361}, \frac{267\,498\,811\,958\,475\,801\,600\,000}{7\,774\,159\,141}\right),$$

and the X-coordinates of rational points on (11) generate the subgroup $\langle -2 \cdot 7, -2 \cdot 3 \cdot 13, 2 \cdot 41 \cdot 313 \rangle$ in $\boldsymbol{Q}/\boldsymbol{Q}^{*2}$. But $m^4 - n^4 \equiv 313 \bmod \boldsymbol{Q}^{*2}$, and again (13) cannot be satisfied.

At $(m,n) = (25,4)$, when the rational rank equals 2, we have two independent points of infinite order given by

$$Q_1 = (3\,635\,678\,235\,000, 6\,993\,942\,635\,796\,480\,000)$$

and

$$Q_2 = \left(\frac{-1\,820\,276\,042\,928\,575\,407\,323\,183\,771\,877\,317\,142\,780\,056\,200}{55\,724\,513\,900\,353\,341\,972\,256\,447\,815\,557\,761},\right.$$
$$\left.\frac{437\,071\,416\,584\,945\,156\,840\,521\,429\,545\,092\,289\,388\,880\,459\,787\,536\,364\,506\,163\,200\,000}{13\,154\,351\,212\,525\,643\,989\,055\,597\,374\,041\,075\,539\,422\,615\,207\,939\,009}\right),$$

which are found to generate $E_{25,4}(\boldsymbol{Q})/2E_{25,4}(\boldsymbol{Q})$. The X-coordinates are, respectively,

$$2 \cdot 3 \cdot 29 \bmod \boldsymbol{Q}^{*2} \quad \text{and} \quad -2 \cdot 409 \bmod \boldsymbol{Q}^{*2}.$$

The torsion group comprises 2-torsion only, and the points

$$T_1 = (-32\,711\,704\,200, 0) \quad \text{and} \quad T_2 = (-31\,932\,184\,200, 0)$$

https://doi.org/10.1017/S0013091507000065 Published online by Cambridge University Press

have X-coordinates satisfying

$$X \equiv -2, -2 \cdot 3 \cdot 7 \cdot 29 \cdot 409 \cdot 641 \bmod \boldsymbol{Q}^{*2}.$$

Thus, (13), which is $X \equiv 3 \cdot 7 \cdot 29 \cdot 641 \bmod \boldsymbol{Q}^{*2}$, is satisfied precisely when

$$\begin{aligned} P &\equiv Q_2 + (-31\,932\,184\,200, 0) \\ &= \Big(\frac{156\,621\,682\,934\,960\,193\,363\,570\,947\,330\,888\,095\,902\,350\,400}{78\,068\,842\,846\,561\,824\,532\,968\,350\,002\,366\,849}, \\ &\qquad \frac{33\,537\,139\,059\,626\,334\,087\,800\,531\,875\,442\,605\,725\,158\,063\,336\,289\,135\,993\,539\,544\,024\,000}{21\,813\,060\,971\,965\,769\,188\,526\,151\,969\,957\,354\,308\,386\,430\,268\,471\,743}\Big) \\ &\qquad \bmod 2E_{25,4}(\boldsymbol{Q}). \end{aligned}$$

And indeed, this point leads to a solution of our problem with (a, b, c, d) at (4) given by

$$\begin{aligned} (a, b, c, d) = (&718\,803\,927\,366\,095\,917\,605, 500\,758\,454\,880\,119\,701, \\ &745\,868\,007\,106\,234\,404\,235, 1\,397\,040\,110\,792\,831\,035). \end{aligned}$$

The sides of the corresponding triangle are

$$\left\{ \begin{aligned} &\frac{47\,543\,925\,293\,556\,151\,140\,577\,725\,151\,441\,411\,041}{49\,549\,997\,534\,627\,550\,167\,697\,846\,720\,148\,046\,249}, \\ &\qquad \frac{15\,613\,768\,569\,312\,364\,906\,593\,670\,000\,473\,369\,800}{49\,549\,997\,534\,627\,550\,167\,697\,846\,720\,148\,046\,249}, \\ &\qquad\qquad \frac{50\,042\,128\,264\,646\,129\,525\,632\,712\,351\,517\,150\,209}{49\,549\,997\,534\,627\,550\,167\,697\,846\,720\,148\,046\,249} \end{aligned} \right\} \tag{14}$$

with

$$\begin{aligned} \text{side}(1) - 2\ \text{area} &= \left(\frac{40\,167\,916\,733\,034\,108\,507\,886\,671\,472\,561\,874\,847}{49\,549\,997\,534\,627\,550\,167\,697\,846\,720\,148\,046\,249}\right)^2, \\ \text{side}(2) - 2\ \text{area} &= \left(\frac{5\,596\,637\,178\,289\,354\,463\,726\,505\,707\,741\,764\,280}{49\,549\,997\,534\,627\,550\,167\,697\,846\,720\,148\,046\,249}\right)^2, \\ \text{side}(3) - 2\ \text{area} &= \left(\frac{41\,680\,300\,931\,380\,871\,913\,026\,881\,740\,489\,737\,329}{49\,549\,997\,534\,627\,550\,167\,697\,846\,720\,148\,046\,249}\right)^2. \end{aligned}$$

There remains the case of $(m, n) = (17, 12)$, satisfying $m + n = 25 + 4$. The rank of $E_{17,12}$ is again 2, and we find generators of $E_{17,12}(\boldsymbol{Q})/2E_{17,12}(\boldsymbol{Q})$ to be

$$Q_1 = (-210\,562\,271, 2\,386\,360\,978\,807)$$

and

$$\begin{aligned} Q_2 = \Big(&\frac{-2\,162\,768\,866\,232\,219\,585\,848\,076\,098\,258\,739\,375}{187\,703\,847\,568\,753\,233\,937\,230\,498\,601}, \\ &\frac{323\,043\,702\,111\,636\,816\,646\,038\,721\,644\,366\,892\,757\,924\,415\,107\,820\,840\,625}{81\,322\,320\,464\,726\,588\,106\,430\,666\,596\,198\,281\,589\,076\,651}\Big). \end{aligned}$$

https://doi.org/10.1017/S0013091507000065 Published online by Cambridge University Press

Arguing as above, (13) is satisfied precisely when

$$\begin{aligned}P &\equiv Q_2 + (0,0)\\ &= \biggl(\frac{1\,961\,775\,921\,090\,588\,853\,308\,172\,341\,694\,752\,306\,240}{15\,645\,100\,147\,712\,759\,739\,025\,701\,601},\\ &\qquad \frac{84\,596\,648\,065\,284\,406\,200\,412\,585\,864\,524\,541\,752\,077\,607\,212\,866\,970\,798\,400}{1\,956\,894\,989\,484\,216\,993\,480\,369\,985\,257\,577\,514\,768\,849}\biggr)\\ &\qquad\qquad \bmod 2E_{17,12}(\boldsymbol{Q}).\end{aligned}$$

This leads to (a,b,c,d) at (4) being given by

$$(102\,508\,212\,978\,445\,855, 433\,248\,020\,848\,051, 182\,255\,935\,472\,405\,617, 125\,080\,374\,750\,449).$$

The sides of the corresponding triangle are

$$\begin{aligned}\biggl\{&\frac{2\,268\,539\,521\,418\,350\,162\,158\,726\,732\,145}{78\,851\,709\,329\,469\,669\,608\,548\,770\,161\,353},\\ &\qquad \frac{6\,383\,200\,860\,266\,805\,973\,522\,486\,253\,208}{78\,851\,709\,329\,469\,669\,608\,548\,770\,161\,353},\\ &\qquad\qquad \frac{6\,774\,328\,363\,959\,624\,966\,998\,128\,793\,233}{78\,851\,709\,329\,469\,669\,608\,548\,770\,161\,353}\biggr\},\end{aligned} \tag{15}$$

with

$$\begin{aligned}\text{side}(1) - 2\text{ area} &= \left(\frac{12\,821\,765\,694\,342\,847\,403\,611\,483\,438\,895}{78\,851\,709\,329\,469\,669\,608\,548\,770\,161\,353}\right)^2,\\ \text{side}(2) - 2\text{ area} &= \left(\frac{22\,109\,856\,521\,486\,340\,581\,376\,994\,158\,792}{78\,851\,709\,329\,469\,669\,608\,548\,770\,161\,353}\right)^2,\\ \text{side}(3) - 2\text{ area} &= \left(\frac{22\,796\,640\,709\,382\,145\,773\,392\,080\,872\,033}{78\,851\,709\,329\,469\,669\,608\,548\,770\,161\,353}\right)^2.\end{aligned}$$

Thus, the right triangles giving a solution to Ozanam's problem, with minimum sum of standard generators (m,n), are those given at (14), (15), occurring for $(m,n) = (25,4)$, $(17,12)$.

References

1. W. Bosma, J. Cannon and C. Playoust, The Magma algebra system, I, The user language, *J. Symb. Computat.* **24** (1997), 235–265.
2. L. E. Dickson, *History of the theory of numbers*, Volume 2, Chapter 4 (Chelsea, New York, 1971).
3. A. Macleod, On a problem from Dickson's history, Number Theory Archives (available at http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind9704&L=nmbrthry&T=0&P=1428).
4. J. Ozanam, *Nouveaux élémens d'algèbre, ou principes généraux, pour résoudre toutes sortes de problèmes de mathématique*, p. 604 (Georges Gallet, Amsterdam, 1702).

https://doi.org/10.1017/S0013091507000065 Published online by Cambridge University Press