<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>A Diophantine equation arising from tight 4-designs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Bremner, Andrew</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Journal of Mathematics. 16(2) P.353-P.356</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1979</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/8744">https://doi.org/10.18910/8744</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/8744</td>
</tr>
<tr>
<td><strong>rights</strong></td>
<td></td>
</tr>
</tbody>
</table>

*Osaka University Knowledge Archive: OUKA*

http://ir.library.osaka-u.ac.jp/dspace/

Osaka University
A DIOPHANTINE EQUATION ARISING FROM TIGHT 4-DESIGNS

ANDREW BREMNER

(Received July 5, 1978)

Ito [1,2] and Enomoto, Ito, Noda [3] show that there exist only finitely many tight 4-designs, by proving that such a design gives rise to a unique rational integral solution of the diophantine equation

\[(2y^2-3x^2-2) = x^2(3x^2-2) \quad (1)\]

and then invoking a result of Mordell [4] to say that this equation has only finitely many solutions in integers \(x,y\). A privately communicated conjecture is that (1) has only the 'obvious' solutions \((\pm x, \pm y) = (1,1), (3,3)\), with the implication that the only tight 4-designs are the Witt designs. We show here that this is indeed the case.

We are exclusively interested in integral points on the curve (1), which is a lightly disguised elliptic curve; standard arguments show that the group of rational points has one generator of infinite order which may be taken to be \((3,3)\).

Suppose now that \(x, y\) are integers satisfying (1). Then there is an integer \(w\) with

\[
\begin{align*}
3x^2-2 &= w^2 \\
2y^2-3 &= wx.
\end{align*}
\]

(2)

Clearly \(x, w, y\) are odd. Following Cassels [5] we write (2), in virtue of the identity \(w^2-3x^2+2wx\sqrt{-3} = (w+x\sqrt{-3})^2\), in the form

\[
\left(\frac{w+x\sqrt{-3}}{2}\right)^2 - y^2\sqrt{-3} = \frac{-1-3\sqrt{-3}}{2} \quad (3)
\]

We now work in the algebraic number field \(Q(\theta)\) where \(\theta^2 = \sqrt{-3}\). It is easy to check that the ring of integers of \(Q(\theta)\) has \(\mathbb{Z}\)-basis \(\{1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2}\}\), that the class-number is 1, and that the group of units is generated by \(\{-\omega, \omega+\theta\}\) where \(\omega = \frac{-1-\theta^2}{2}\) is a cube root of unity. The relative norm to \(Q(\sqrt{-3})\) of
the fundamental unit $\varepsilon = \omega + \theta$, is $\omega$.

Further, $-1 - 3\sqrt{-3}$ is prime in $\mathbb{Z}[^{\omega}]$, and splits into two first degree primes in $\mathbb{Q}(\theta)$:

$$-\frac{1 - 3\sqrt{-3}}{2} = (1 - \frac{1}{2}\theta - \theta^2 - \frac{1}{2}\theta^3)(1 + \frac{1}{2}\theta - \theta^2 + \frac{1}{2}\theta^3).$$

Now the left hand side of (3) is the product of the two factors $\frac{w - x\sqrt{-3}}{2}$ $\pm y\theta$ conjugate over $\mathbb{Q}(\sqrt{-3})$, so by unique factorisation we deduce that

$$\frac{w + x\theta^2}{2} + y\theta = \eta(1 - \theta^2 \pm \frac{1}{2}\theta(1 + \theta^2))$$

where $\eta$ is a unit of $\mathbb{Q}(\theta)$ with relative norm 1 - the possibilities for $\eta$ are $\pm \varepsilon^{3m}$, $\pm \omega\varepsilon^{3m+1}$, $\pm \omega^2\varepsilon^{3m+2}$, for some integer $m$. By changing the sign of $y$ if necessary, we may thus assume that

$$\pm\left(\frac{w + x\theta^2}{2} + y\theta\right) = (\omega\varepsilon^i(1 + \frac{1}{2}\theta - \theta^2 + \frac{1}{2}\theta^3))E^m \quad (4)$$

where $i = 0, 1, 2$ and $E = \varepsilon^3 = \frac{1}{2}(11 - 3\theta - 3\theta^2 + 5\theta^3)$.

Write (4) as

$$\pm\left(\frac{w + x\theta^2}{2} + y\theta\right) = \lambda E^m$$

where $\lambda$ is one of three possibilities,

$$\lambda_1 = 1 + \frac{1}{2}\theta - \theta^2 + \frac{1}{2}\theta^3$$

$$\lambda_2 = \frac{5}{2} - 3\theta + \frac{3}{2}\theta^2$$

$$\lambda_3 = -8 + \frac{5}{2}\theta + 2\theta^2 - \frac{7}{2}\theta^3.$$

We now choose to work 37-adically.

Since $E^n \equiv -1 \mod 37$, we have upon putting $m = 6n + r$, $0 \leq r \leq 5$,

$$\pm\left(\frac{w + x\theta^2}{2} + y\theta\right) = \lambda E'(1 - 37\xi)^n$$

where $\xi$ is an integer of $\mathbb{Q}(\theta)$ which by direct calculation satisfies $\xi \equiv -15\theta - 5\theta^3 \mod 37$.

Accordingly, we require that the coefficient of $\frac{\theta + \theta^3}{2}$ in $\lambda E^r$ be congruent
to zero modulo 37: and this is clearly equivalent to the coefficient of $\theta^3$ being zero modulo 37.

From the following table we deduce that $\lambda E^r$ can only be $\lambda_2$ or $\lambda_3 E^{-1}$ (absorbing an $E^6$ into $E^6n$ for convenience) where $\lambda_3 E^{-1} = -\frac{1}{2} + \theta + \frac{1}{2} \theta^2$. Coefficient modulo 37 of $\theta^3$ in $\lambda_3 E^r$:

<table>
<thead>
<tr>
<th>$r$</th>
<th>$1$</th>
<th>$2$</th>
<th>$3$</th>
<th>$4$</th>
<th>$5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda_1 E^r$</td>
<td>19</td>
<td>6</td>
<td>14</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>$\lambda_2 E^r$</td>
<td>0</td>
<td>27</td>
<td>3</td>
<td>30</td>
<td>27</td>
</tr>
<tr>
<td>$\lambda_3 E^r$</td>
<td>15</td>
<td>28</td>
<td>12</td>
<td>20</td>
<td>18</td>
</tr>
</tbody>
</table>

In the case that $\lambda = \lambda_2$ we have

$$\pm \left( \frac{w + x \theta^2}{2} + y \theta \right) = \left( \frac{5}{2} - 3 \theta + \frac{3}{2} \theta^2 \right) (1 + 37 \xi)^r$$

One can treat this exponential equation in the manner of Skolem [6], but it is preferable to argue directly. Suppose in (5) that $n \neq 0$, and let the highest power of 37 that divides $n$, be $s$.

Now $$(1 + 37 \xi)^n = 1 + 37n \xi + 37^2(\xi)^2 + \cdots$$

$$\equiv 1 + 37n \xi \mod 37^{s+2}$$

$$\equiv 1 + 37n(-15\theta - 5\theta^3) \mod 37^{s+2}.$$

So equating to zero the coefficient of $\theta^3$ on the right hand side of (5) we obtain

$$0 \equiv \frac{5}{2} (-5n.37) + \frac{3}{2} (-15n.37) \mod 37^{s+2}$$

i.e. $0 \equiv -35n.37 \mod 37^{s+2}$, contradiction.

Hence $n=0$ is the only possibility for a solution in (5), and it does indeed result in $(x,y) = (3, -3)$.

The case $\lambda = \lambda_3 E^{-1}$ is treated in precisely the same way, resulting in the single solution $(x,y) = (1,1)$.

We have thus shown that the only integer solutions of (1) are indeed given by $(\pm x, \pm y) = (1,1), (3,3)$.

EMMANUEL COLLEGE, CAMBRIDGE

References