

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

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

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

$$\begin{aligned} 3x^2-2 &= w^2 \\ 2y^2-3 &= wx. \end{aligned} \quad (2)$$

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 \mathbf{Z} -basis $\left\{1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2}\right\}$, 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 ω .

Further, $\frac{-1-3\sqrt{-3}}{2}$ is prime in $\mathbf{Z}[\omega]$, and splits into two first degree primes in $Q(\theta)$:

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

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 $Q(\sqrt{-3})$, 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 η is a unit of $Q(\theta)$ with relative norm 1 - the possibilities for η 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

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

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 λ is one of three possibilities,

$$\begin{aligned} \lambda_1 &= 1 + \frac{1}{2}\theta - \theta^2 + \frac{1}{2}\theta^3 \\ \lambda_2 &= \frac{5}{2} - 3\theta + \frac{3}{2}\theta^2 \\ \lambda_3 &= -8 + \frac{5}{2}\theta + 2\theta^2 - \frac{7}{2}\theta^3. \end{aligned}$$

We now choose to work 37-adically.

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

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

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

Accordingly, we require that the coefficient of $\frac{\theta+\theta^3}{2}$ in λE^r be congruent

to zero modulo 37: and this is clearly equivalent to the coefficient of θ^3 being zero modulo 37.

From the following table we deduce that λE^r can only be λ_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 θ^3 in $\lambda_i E^r$:-

	$r=0$	1	2	3	4	5
$\lambda_1 E^r$	19	6	14	13	1	2
$\lambda_2 E^r$	0	27	3	30	27	18
$\lambda_3 E^r$	15	28	12	20	18	0

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

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

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 .

$$\begin{aligned} \text{Now } (1+37\xi)^n &= 1 + 37n\xi + 37^2 \binom{n}{2} \xi^2 + \dots \\ &\equiv 1 + 37n\xi \pmod{37^{s+2}} \\ &\equiv 1 + 37n(-15\theta - 5\theta^3) \pmod{37^{s+2}}. \end{aligned}$$

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

$$\begin{aligned} 0 &\equiv \frac{5}{2}(-5n \cdot 37) + \frac{3}{2}(-15n \cdot 37) \pmod{37^{s+2}} \\ \text{i.e. } 0 &\equiv -35n \cdot 37 \pmod{37^{s+2}}, \text{ contradiction.} \end{aligned}$$

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

[1] N. Ito: *On tight 4-designs*, Osaka J. Math. **12** (1975), 493-522.

- [2] N. Ito: *Corrections and supplement to "On tight 4-designs"*, Osaka J. Math. **15** (1978), 693–697.
- [3] H. Enomoto, N. Ito, R. Noda: *Tight 4-designs*, Osaka J. Math. **16** (1979), 39–43.
- [4] L.J. Mordell: *Diophantine equations*, Academic Press, 1969, p. 276.
- [5] J.W.S. Cassels: *Integral points on certain elliptic curves*, Proc. London Math. Soc. (3) **14A** (1965), 55–57.
- [6] Th. Skolem: *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen*, 8de Skand. mat. Kongr. Forh. Stockholm, 1934.