On Oranges and Integral Points on certain Plane Cubic Curves

Frits Beukers and Jaap Top*
Mathematisch Instituut, Rijksuniversiteit Utrecht
Budapestlaan 6, 3508 TA Utrecht, The Netherlands

1. Introduction

On a number theory day held at the University of Utrecht in the spring of 1987, the Belgian mathematician M. Coppens came with the following problem:

'A greengrocer wanted to attract customers by displaying a huge pyramid built from oranges in front of his shop. Unfortunately he and his wife disagreed on the form of this pyramid; one of them thought that the base of it should be a square while the other argued that a triangular base would have much more effect. At last they decided to buy an amount of oranges such that it would be possible to build either the square or the triangular pyramid out of it. How many oranges should this greengrocer buy?'

It is easily seen that this question leads to the problem of finding all integral points on a certain smooth plane cubic curve. In general this is a very hard problem: as far as we know there isn't even an algorithm which determines whether a given curve of this kind has any rational points. In our situation however there are rational (and even integral) points, for instance the point corresponding to a pyramid consisting of only one orange. This makes it possible to regard the curve in question as an elliptic curve. The rational points on any elliptic curve are known to constitute a finitely generated abelian group (Mordell-Weil theorem); in our situation it turns out that this is an infinite cyclic group. We even know a generator of this group. Unfortunately, even with this knowledge it is not at all obvious how to find all integral points on our model of this elliptic curve; on the one hand it is not given by a Weierstrass equation; on the other hand, even for Weierstrass equations it is quite hard (see e.g. [5]).

* Supported by NWO.

It turns out that in the case we are dealing with there exists a second, more successful approach to the problem. One can show that each integral solution of the equation we are dealing with gives rise to an integral solution of the inequality $|x^3 - 2y^3| \leqslant 30$. This inequality can be solved completely using a theorem of D. Easton [2] and the remark that any solution yields a very good rational approximation to $\sqrt[3]{2}$.

With regard to the greengrocer, we have the following rather unpleasant fact:

THEOREM 1. *No integer greater than 1 equals both the number of oranges in a pyramid with a square base and the number of oranges in a pyramid with a triangular base.*

In the next section of this paper the diophantine equation corresponding to this problem is given; it is transformed into a Weierstrass equation and some results from the arithmetic theory of elliptic curves are used in order to determine the group of rational points on the curve given by it. The only reason to include this here is that it provides a nice example how certain aspects of this theory work; it is not used in Section 3 where the proof of our theorem will be given.

We like to thank Herman te Riele for checking some computer calculations we used and for pointing out an error which occurred in an earlier version of this paper.

2. THE ELLIPTIC CURVE INVOLVED

The problem stated in Section 1 is that of finding a (non-trivial) pair (x,y) of positive integers satisfying

$$\sum_{i=1}^{y} i^2 = \sum_{i=1}^{x} \frac{1}{2} i(i+1) \tag{1}$$

or, equivalently,

$$(2y+1)(y+1)y = x(x+1)(x+2). \tag{2}$$

It is easily verified that the corresponding homogeneous equation defines a smooth complete curve of genus 1 in $\mathbb{P}^2$ (even in all characteristics different from 3 and 5). Any curve C of this type is isomorphic to a curve given by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where everything can be defined over any field K for which the set $C(K)$ of K-rational points on C is not empty (see e.g. [3], Chapter III, Proposition 3.1). This is done by first choosing a K-rational point P on C, then choosing rational functions x,y on C defined over K having a pole of order 2, 3 respectively in P and no other poles and using these to define an embedding of C in $\mathbb{P}^2$. After some rescaling this yields the desired model of C. This method works by virtue of the Riemann-Roch theorem which implies in our situation that the vector space over K of rational functions on C defined over K having a pole in the point P of order at most $n>0$ and no other poles, has dimension n.

In case the curve of genus 1 is given by a plane model it is quite easy to give such functions needed to find a Weierstrass equation explicitly. For the curve we are dealing with the following trivial lemma can be used:

LEMMA 1. *The point with coordinates* $(x,y)=(-1,-\frac{1}{2})$ *is a flex on the curve given by equation* (2). *The tangent line to the curve through this point is given by* $4x-2y+3=0$.

This lemma implies that $\xi=\frac{x-2y}{4x-2y+3}$ and $\eta=\frac{x}{4x-2y+3}$ are functions as wanted. What remains to be done is finding a relation of the form

$$\eta^2 + a_1\eta\xi + a_3\eta = \lambda\xi^3 + a_2\xi^2 + a_4\xi$$

between them (there is no constant term because both functions are zero in the point (0,0) of the original curve). This boils down to writing the occurring monomials in ξ and η in the form $\frac{1}{(4x-2y+3)^3}$ times a polynomial in x and y and substituting this in a relation as above. One then solves the system of linear equations in the a_i's and λ obtained by comparing coefficients of the occurring monomials in x and y. The result of this computation is:

PROPOSITION 1. *The functions* $\xi=\frac{x-2y}{4x-2y+3}$ *and* $\eta=\frac{x}{4x-2y+3}$ *on the curve given by equation* (2) *are related by*

$$\eta^2 + \frac{2}{3}\xi\eta - \frac{2}{3}\eta = \frac{20}{9}\xi^3 - \frac{13}{9}\xi^2 + \frac{2}{9}\xi. \qquad (3)$$

The equation we just found can be transformed into a Weierstrass equation by replacing ξ and η by $X=20\xi-4$ and $Y=60\eta+20\xi-20$, respectively. One finds that X and Y satisfy the simple relation

$$Y^2 = X^3 - 48X + 272.$$

In fact we have shown:

PROPOSITION 2. *The curve given by equation* (2) *is isomorphic over* $\mathbb{Q}$ *to the elliptic curve given by* $y^2=x^3-48x+272$.

We write E for the elliptic curve given by $y^2=x^3-48x+272$. The set of points on E with coordinates in $\mathbb{Q}$ will be regarded in the usual way (see e.g. [3], Chapter III, §2) as an abelian group denoted by $E(\mathbb{Q})$. A simple search for integers m such that $m^3-48m+272$ is a square yields the following elements $P_i \in E(\mathbb{Q})$: $P_1=(-8,12), P_2=(-4,20)$, $P_3=(1,15), P_4=(4,12)$, $P_5=(8,20)$ and $P_6=(16,60)$. To find relations between the points P_i one may look for lines intersecting E in at least two of them. For example, the line given by

$y=12$ intersects E in P_1 and is tangent to E in P_4; this gives the relation $P_1+2P_4=0$. Computing like this for some time one finds that every P_i is a multiple of P_6: $P_1=-4P_6$, $P_2=3P_6$, $P_3=-5P_6$, $P_4=2P_6$ and $P_5=-6P_6$. By trying more multiples of P_6 it turns out that there are even more integral points on $E: 7P_6=(76,-660)$ and $8P_6=(52,372)$. The next 4 multiples of P_6 don't give integral points. This can be verified by a trivial computation. For $11P_6$ it also follows by remarking that P_5 and $-P_3$ define the same point in characteristic 7. Because our equation also defines a smooth curve modulo 7 it follows that $11P_6=-P_3-P_5$ is the trivial point there. This implies that over $\mathbf{Q}$ the coordinates of $11P_6$ have a denominator divisible by 7 (unless P_6 should have order 11 which it has not since $5P_6\neq -6P_6$; see also [3], Chapter VIII, Theorem 7.5).

The computation of generators for such a group $E(\mathbf{Q})$ in specific examples is usually lengthy and not very illuminating. In fact it is not even known whether a method exists which is guaranteed to give generators in a finite amount of time. In our case we are lucky since the curve we are looking at already appears in the literature.

PROPOSITION 3. *The group $E(\mathbf{Q})$ of $\mathbf{Q}$-rational points on the elliptic curve E given by the equation*

$$y^2=x^3 - 48x + 272$$

is an infinite cyclic group generated by the point with coordinates $(x,y)=(16,60)$.

To prove this we only have to remark that the transformation $\eta=\frac{1}{8}y-\frac{1}{2}, \xi=\frac{1}{4}x$ puts our equation in the form

$$\eta^2 + \eta = \xi^3 - 3\xi + 4$$

which defines the elliptic curve listed as 135A in [1]. We read from the tables that its group of rational points is generated by $(\xi,\eta)=(4,7)$ which corresponds to $(x,y)=(16,60)$. The fact that the torsion subgroup of $E(\mathbf{Q})$ is trivial can be seen from these tables; it also follows from the fact that reduction modulo prime numbers defines an injective homomorphism

$$E(\mathbf{Q})_{tors}\rightarrow E(F_p)$$

unless $p=2$ in which case the kernel may contain points of order 2 (see [3], Chapter VII, Theorem 3.4). Using the model E_1 defined by the equation in ξ and η one computes $\#E_1(F_2)=5$ and $\#E_1(F_7)=11$, so the fact above implies that $E(\mathbf{Q})$ contains no non-trivial points of finite order.

3. THE SOLUTION OF THE ORANGE PROBLEM

As stated in the beginning of Section 2 we have to find non-trivial solutions in positive integers of the equation

$$(2y+1)(y+1)y=x(x+1)(x+2).$$

PROPOSITION 4. *From any pair of integers satisfying* $(2y+1)(y+1)y = x(x+1)(x+2)$ *one can derive an integral solution of* $X^3-2Y^3 \in \{-2, -6, -10, -30\}$.

PROOF. Writing $2y+1=k$ and $x+1=n$ the equation becomes

$$k^3 - 4n^3 = k - 4n$$

which must be solved with k odd. It is now natural to look at $l=k-4n$. Substituting $k=l+4n$ one is left with

$$(l+4n)^3 - 4n^3 = l.$$

The following lemma can be applied.

LEMMA 2. *Suppose* l *and* n *are integers satisfying* $(l+4n)^3-4n^3=l$. *Then* $l/\gcd(60,l)$ *is a perfect cube.*

PROOF OF THE LEMMA. Given l and n as in the lemma, write $d=\gcd(60,l)$. Let p be a prime number and write v_p for the valuation at p. It follows by reduction modulo l that $60n^3=(4n)-4n^3\equiv 0 \pmod l$, so $\frac{l}{d}$ divides n^3. In fact the equation implies that $\frac{60}{d}n^3=\frac{1}{d}(1-l^2-12ln-48n^2)$; hence, if $v_p(\frac{l}{d})>0$ then $v_p(\frac{l}{d})=v_p(n^3)=3v_p(n)$.

By the lemma, given a solution of $(l+4n)^3-4n^3=l$, one can find an integer u such that $\frac{l}{\gcd(60,l)}=u^3$. In the proof of the lemma we also saw that u^3 divides n^3; hence, we can write $n=uv$ for an integer v. Rewriting everything in terms of u and v we obtain

$$(\gcd(60,l)u^3+4uv)^3 - 4u^3v^3 = \gcd(60,l)u^3.$$

The trivial solution $u=0$ is of no interest since it leads to $l=0$ which does not give an integral solution of our original equation. Hence, division by u^3 is allowed; what is left is an equation

$$(\gcd(60,l)u^2+4v)^3 - 4v^3 = \gcd(60,l).$$

If we write $X=2v$ and $Y=\gcd(60,l)u^2+4v$ and use that l must be odd, so that $\gcd(60,l)\in\{1,3,5,15\}$, it follows that any integral solution of the equation we started with leads to a pair of integers (X,Y) satisfying $X^3-2Y^3\in\{-2,-6,-10,-30\}$, which is the assertion of our proposition.

We will be looking for all integral solutions of $|x^3-2y^3|\leqslant 30$.

LEMMA 3. *If a pair of integers* (x,y) *satisfies* $|x^3-2y^3|\leqslant 30$, *then either* $|y|\leqslant 300$ *or* $\frac{x}{y}$ *is a convergent in the continued fraction expansion of* $\sqrt[3]{2}$.

PROOF. Suppose $|x^3-2y^3|\leqslant 30$ and $|y|>300$. It follows that

$$\left|\frac{30}{y^3}\right|\geqslant\left|\frac{x^3}{y^3}-2\right| = \left|\frac{x}{y}-\sqrt[3]{2}\right|\left(\left(\frac{x}{y}\right)^2 + \sqrt[3]{2}\left(\frac{x}{y}\right) + \sqrt[3]{4}\right).$$

Since $\left|\frac{30}{y^3}\right|<\frac{1}{9\cdot 10^5}$ we have $\frac{x}{y}>1.2599$; hence the inequality $\left(\frac{x}{y}\right)^2+\sqrt[3]{2}\left(\frac{x}{y}\right)+\sqrt[3]{4}>4.7622$ holds. This implies that

$$\left|\frac{x}{y} - \sqrt[3]{2}\right|\leqslant\frac{30}{4.7622}\times\frac{1}{|y|^3}.$$

The theory of continued fractions asserts that such a good approximation of $\sqrt[3]{2}$ must be a convergent (see e.g. [4], Theorem 7.19).

What remains to be done is finding an upperbound for the number of convergents one has to compute. This is provided by

LEMMA 4. *Suppose that a pair of integers* (x,y) *satisfy* $|x^3-2y^3|\leqslant 30$ *and* $|y|>300$. *Then one has* $|y|<10^{45}$.

PROOF. Apply a theorem of D. Easton which says that for integers x and y the inequality

$$\left|\frac{x}{y} - \sqrt[3]{2}\right|>\frac{2.2}{10^8}\times\frac{1}{|y|^{2.795}}$$

holds (see [2], p. 614, Corollary). Combining this with the inequality derived in the proof of the previous lemma we obtain

$$y^{0.205}\leqslant\frac{30}{4.7622}\times\frac{10^8}{2.2}.$$

From this the lemma follows.

At first sight the practical value of this lemma may not be apparent. The reason why it really helps is that the numerators and denominators of the convergents of any irrational number grow exponentially: writing the n-th convergent as $\frac{p_n}{q_n}$ one has $q_n\geqslant q_{n-1}+q_{n-2}$ (see e.g. [4], Theorem 7.7). To compute these convergents for $\sqrt[3]{2}$ one may use the following prescription:

** Put

$$\sqrt[3]{2} = b_0 + \cfrac{1}{b_1+\cfrac{1}{b_2+\dots}} = [b_0, b_1,\dots] \text{ and } \frac{p_n}{q_n} = [b_0,\dots,b_n].$$

** One has

$$b_0=1, b_1=3, p_0 = 1, p_1 = 4, q_0 = 1 \text{ and } q_1 = 3.$$

The p_i and q_i satisfy $p_i=p_{i-2}+b_ip_{i-1}$ and $q_i=q_{i-2}+b_iq_{i-1}$.

** The number b_i is the largest number a for which the sign of

$$(p_{i-2}+ap_{i-1})^3 \ - \ 2(q_{i-2}+aq_{i-1})^3$$

is the same as the sign of $p_{i-2}^3 - 2q_{i-2}^3$.

Using a computer it is very easy to obtain lots of convergents of $\sqrt[3]{2}$. It turns out that we only need the first 82 of them:

$$\frac{p_{81}}{q_{81}} = \frac{11417896481733258063546721914876072708558976077}{906239044318368876405588750186156684296322081}$$

is the last convergent with a denominator smaller than 10^{45}. As a result of the computation one has:

Proposition 5. *Only the first three convergents* $\frac{p}{q}$ *of* $\sqrt[3]{2}$ *satisfy* $|p^3 - 2q^3| \leqslant 30$. *The continued fraction expansion of* $\sqrt[3]{2}$ *begins as*

$$[1,3,1,5,1,1,4,1,1,8,1,14,1,10,2,1,4,12,2,3,2,1,3,4,1,1,2,14,$$

$$3,12,1,15,3,1,4,534,1,1,5,1,1,121,1,2,2,4,10,3,2,2,41,1,1,$$

$$1,3,7,2,2,9,4,1,3,7,6,1,1,2,2,9,3,1,1,69,4,4,5,12,1,1,5,15,1, \ldots].$$

The problem of finding all integral solutions of $|X^3 - 2Y^3| \leqslant 30$ is now reduced to searching for solutions with $|Y| \leqslant 300$; by performing this search it follows that in fact all solutions satisfy $|Y| \leqslant 8$. With regard to the orange problem, the only solutions in (X, Y) are $(0,1), (-2,-1), (-4,-3)$ and $(-2,1)$. By tracing through all the transformations this implies:

Proposition 6. *The following list contains all pairs of integers* (x,y) *satisfying the equation* $(2y+1)(y+1)y = x(x+1)(x+2)$:

$$(-3,-2)\ (-2,-1)\ (-2,0)\ (-1,-1)\ (-1,0)\ (0,-1)\ (0,0)\ (1,1).$$

If one wants to think of all transformations given in the beginning of this section in a geometric way, it works as follows. Let C_t be the family of curves of arithmetic genus 10 parametrized by t, given by the equation

$$(2v)^3 \ - \ 2(tu^2+4v)^3 \ = \ -2t.$$

This family maps via $X=2v$, $Y=tu^2+4v$ down to a family of curves of genus 1 (and constant j-invariant) given by $X^3 - 2Y^3 = -2t$. The substitution $tu^3 = l$ and $uv = n$ we used means that we also have a map from C_t to the curve D given by $(l+4n)^3 - 4n^3 = l$. Every integral point on D can be lifted to an integral point on some fiber of C_t and is then mapped to an integral point in a fiber of the given family of curves of genus 1. By trivial considerations it turns out that it is possible to limit the number of fibers in which our integral point could land.

References

1. B. Birch and W. Kuyk, 1975, *Modular functions of one variable IV,* Springer-Verlag, LNM 476.
2. D. Easton, 1986, *Effective irrationality measures for certain algebraic numbers,* Math. of Comp., **46,** pp. 613-622.
3. J.H. Silverman, 1986, *The arithmetic of elliptic curves,* Springer-Verlag, GTM 106.
4. H.M. Stark, 1970, *An introduction to number theory,* Markham Publishing Company.
5. D. Zagier, 1987, *Large integral points on elliptic curves,* Math. of Comp., **48,** pp. 425-436.