

TRIANGLES WITH TWO INTEGRAL SIDES

SZ. TENGELY

ABSTRACT. We study some Diophantine problems related to triangles with two given integral sides. We solve two problems posed by Zoltán Bertalan and we also provide some generalization.

1. INTRODUCTION

There are many Diophantine problems arising from studying certain properties of triangles. Most people know the theorem on the lengths of sides of right angled triangles named after Pythagoras. That is $a^2 + b^2 = c^2$.

An integer $n \geq 1$ is called congruent if it is the area of a right triangle with rational sides. Using tools from modern arithmetic theory of elliptic curves and modular forms Tunnell [10] found necessary condition for n to be a congruent number. Suppose that n is a squarefree positive integer which is a congruent number.

- (a) If n is odd, then the number of integer triples (x, y, z) satisfying the equation $n = 2x^2 + y^2 + 8z^2$ is just twice the number of integer triples (x, y, z) satisfying $n = 2x^2 + y^2 + 32z^2$.
- (b) If n is even, then the number of integer triples (x, y, z) satisfying the equation $\frac{n}{2} = 4x^2 + y^2 + 8z^2$ is just twice the number of integer triples (x, y, z) satisfying $\frac{n}{2} = 4x^2 + y^2 + 32z^2$.

A Heronian triangle is a triangle having the property that the lengths of its sides and its area are positive integers. There are several open problems concerning the existence of Heronian triangles with certain properties. It is not known whether there exist Heronian triangles having the property that the lengths of all their medians are positive integers [6], and it is not known whether there exist Heronian triangles having the property that the lengths of all their sides are Fibonacci numbers [7]. Gaál, Járási and Luca [5] proved that there are only finitely many Heronian triangles whose sides $a, b, c \in S$ and are reduced, that is $\gcd(a, b, c) = 1$, where S denotes the set of integers divisible only by some fixed primes.

Petulante and Kaja [9] gave arguments for parametrizing all integer-sided triangles that contain a specified angle with rational cosine. It is equivalent to determining a rational parametrization of the conic $u^2 - 2\alpha uv + v^2 = 1$, where α is the rational cosine.

The present paper is motivated by the following two problems due to Zoltán Bertalan.

- (i) How to choose x and y such that the distances of the clock hands at 2 o'clock and 3 o'clock are integers?
- (ii) How to choose x and y such that the distances of the clock hands at 2 o'clock and 4 o'clock are integers?

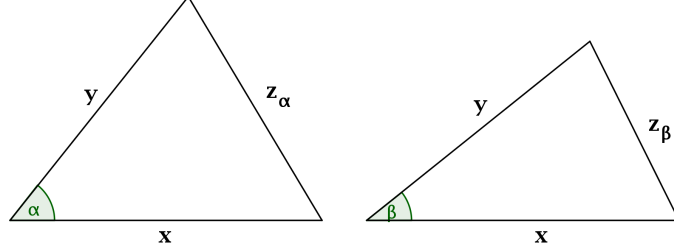
We generalize and reformulate the above questions as follows. For given $0 < \alpha, \beta < \pi$ we are looking for pairs of triangles in which the length of the sides

2000 *Mathematics Subject Classification.* Primary 11D61; Secondary 11Y50.

Key words and phrases. Diophantine equations, Elliptic curves.

Research supported in part by the Magyar Zoltán Higher Educational Public Foundation.

(z_α, z_β) opposite the angles α, β are from some given number field $\mathbb{Q}(\theta)$ and the length of the other two sides (x, y) are rational integers. Let $\varphi_1 = \cos(\alpha)$ and $\varphi_2 = \cos(\beta)$.



By means of the law of cosine we obtain the following systems of equations

$$\begin{aligned} x^2 - 2\varphi_1 xy + y^2 &= z_\alpha^2, \\ x^2 - 2\varphi_2 xy + y^2 &= z_\beta^2, \end{aligned}$$

After multiplying these equations and dividing by y^4 we get

$$\mathcal{C}_{\alpha, \beta} : X^4 - 2(\varphi_1 + \varphi_2)X^3 + (4\varphi_1\varphi_2 + 2)X^2 - 2(\varphi_1 + \varphi_2)X + 1 = Y^2,$$

where $X = x/y$ and $Y = z_\alpha z_\beta / y^2$. Suppose $\varphi_1, \varphi_2 \in \mathbb{Q}(\theta)$ for some algebraic number θ . Clearly, the hyperelliptic curve $\mathcal{C}_{\alpha, \beta}$ has a rational point $(X, Y) = (0, 1)$, so it is isomorphic to an elliptic curve $\mathcal{E}_{\alpha, \beta}$. The rational points of an elliptic curve form a finitely generated group. We are looking for points on $\mathcal{E}_{\alpha, \beta}$ for which the first coordinate of its preimage is rational. If $\mathcal{E}_{\alpha, \beta}$ is defined over \mathbb{Q} and the rank is 0, then there are only finitely many solutions, if the rank is greater than 0, then there are infinitely many solutions. If the elliptic curve $\mathcal{E}_{\alpha, \beta}$ is defined over some number field of degree at least two, then one can apply the so-called elliptic Chabauty method (see [2, 3] and the references given there) to determine all solutions with the required property.

2. CURVES DEFINED OVER \mathbb{Q}

2.1. $(\alpha, \beta) = (\pi/3, \pi/2)$. The system of equations in this case is

$$\begin{aligned} x^2 - xy + y^2 &= z_{\pi/3}^2, \\ x^2 + y^2 &= z_{\pi/2}^2. \end{aligned}$$

The related hyperelliptic curve is $\mathcal{C}_{\pi/3, \pi/2}$.

Theorem 1. *There are infinitely many rational points on $\mathcal{C}_{\pi/3, \pi/2}$.*

Proof. In this case the free rank is 1, as it is given in Cremona's table of elliptic curves [4] (curve 192A1). Therefore there are infinitely many rational points on $\mathcal{C}_{\pi/3, \pi/2}$. \square

Corollary. *Problem (i) has infinitely many solutions.*

Few solutions are given in the following table.

x	y	$z_{\pi/3}$	$z_{\pi/2}$
8	15	13	17
1768	2415	2993	3637
10130640	8109409	9286489	12976609
498993199440	136318711969	517278459169	579309170089

2.2. $(\alpha, \beta) = (\pi/2, 2\pi/3)$. The system of equations in this case is

$$\begin{aligned} x^2 + y^2 &= z_{\pi/2}^2, \\ x^2 + xy + y^2 &= z_{2\pi/3}^2. \end{aligned}$$

The hyperelliptic curve $\mathcal{C}_{\pi/2, 2\pi/3}$ is isomorphic to $\mathcal{C}_{\pi/3, \pi/2}$, therefore there are infinitely many rational points on $\mathcal{C}_{\pi/2, 2\pi/3}$.

2.3. $(\alpha, \beta) = (\pi/3, 2\pi/3)$. We have

$$\begin{aligned} x^2 - xy + y^2 &= z_{\pi/3}^2, \\ x^2 + xy + y^2 &= z_{2\pi/3}^2. \end{aligned}$$

After multiplying these equations we get

$$(1) \quad x^4 + x^2y^2 + y^4 = (z_{\pi/3}z_{2\pi/3})^2.$$

Theorem 2. *If (x, y) is a solution of (1) such that $\gcd(x, y) = 1$, then $xy = 0$.*

Proof. See [8] at page 19. □

Corollary. *Problem (ii) has no solution.*

In the following sections we use the so-called elliptic Chabauty's method (see [2], [3]) to determine all points on the curves $\mathcal{C}_{\alpha, \beta}$ for which X is rational. The algorithm is implemented by N. Bruin in MAGMA [1], so here we indicate the main steps only, the actual computations can be carried out by MAGMA. The MAGMA code clock.m which were used is given below. It requires three inputs, a, b as members of some number fields and p a prime number.

3. CURVES DEFINED OVER $\mathbb{Q}(\sqrt{2})$

3.1. $(\alpha, \beta) = (\pi/4, \pi/2)$. The hyperelliptic curve $\mathcal{C}_{\pi/4, \pi/2}$ is isomorphic to

$$\mathcal{E}_{\pi/4, \pi/2} : \quad v^2 = u^3 - u^2 - 3u - 1.$$

The rank of $\mathcal{E}_{\pi/4, \pi/2}$ over $\mathbb{Q}(\sqrt{2})$ is 1, which is less than the degree of $\mathbb{Q}(\sqrt{2})$. Applying elliptic Chabauty (the procedure "Chabauty" of MAGMA) with $p = 7$, we obtain that $(X, Y) = (0, \pm 1)$ are the only affine points on $\mathcal{C}_{\pi/4, \pi/2}$ with rational first coordinates. Since $X = x/y$ we get that there does not exist appropriate triangles in this case.

3.2. $(\alpha, \beta) = (\pi/4, \pi/3)$. The hyperelliptic curve $\mathcal{C}_{\pi/4, \pi/3}$ is isomorphic to

$$\mathcal{E}_{\pi/4, \pi/3} : \quad v^2 = u^3 + (\sqrt{2} - 1)u^2 - 2u - \sqrt{2}.$$

The rank of $\mathcal{E}_{\pi/4, \pi/3}$ over $\mathbb{Q}(\sqrt{2})$ is 1 and applying elliptic Chabauty's method again with $p = 7$, we obtain that $(X, Y) = (0, \pm 1)$ are the only affine points on $\mathcal{C}_{\pi/4, \pi/3}$ with rational first coordinates. As in the previous case we obtain that there does not exist triangles satisfying the appropriate conditions.

4. CURVES DEFINED OVER $\mathbb{Q}(\sqrt{3})$ AND $\mathbb{Q}(\sqrt{5})$

In the following tables we summarize some details of the computations, that is the pair (α, β) , the equations of the elliptic curves $\mathcal{E}_{\alpha, \beta}$, the rank of the Mordell-Weil group of these curves over the appropriate number field ($\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{5})$), the rational first coordinates of the affine points and the primes we used.

Algorithm 1 MAGMA code clock.m

```

clock:=function(a,b,p)
P1:=ProjectiveSpace(Rationals(),1);
K1:=Parent(a);
K2:=Parent(b);
if IsIntegral(a) then
  K1:=RationalField();
end if;
if IsIntegral(b) then
  K2:=RationalField();
end if;
if Degree(K1)*Degree(K2) eq 1 then
  K:=RationalField();
else
  if Degree(K1) gt 1 and Degree(K2) gt 1 then
    K:=CompositeFields(K1,K2)[1];
  else
    if Degree(K1) eq 1 then
      K:=K2;
    else
      K:=K1;
    end if;
  end if;
end if;
P<X>:=PolynomialRing(K);
ka:=K!a;
kb:=K!b;
C:=HyperellipticCurve( $X^4 - 2 * (ka + kb) * X^3 + (4 * ka * kb + 2) * X^2 - 2 * (ka + kb) * X + 1$ );
pt:=C![0,1];
E,CtoE:=EllipticCurve(C,pt);
Em,EtoEm:=MinimalModel(E);
umap:=map<C->P1|[C.1,C.3]>;
U:=Expand(Inverse(CtoE*EtoEm)*umap);
RB:=RankBound(Em);
print Em,RB;
if RB ne 0 then
  success,G,mwmap:=PseudoMordellWeilGroup(Em);
  NC,VC,RC,CC:=Chabauty(mwmap,U,p);
  print success,NC,#VC,RC;
  if NC eq #VC then
    print {EvaluateByPowerSeries(U,mwmap(gp)): gp in VC};
    print forall{pr: pr in PrimeDivisors(RC)|IsPSaturated(mwmap,pr)};
  end if;
else
  success,G,mwmap:=PseudoMordellWeilGroup(Em);
  print #G,#TorsionSubgroup(Em);
  print {EvaluateByPowerSeries(U,mwmap(gp)): gp in G};
end if;
return K,C;
end function;

```

(α, β)	$\mathcal{E}_{\alpha, \beta}$	Rank	X	p
$(\pi/6, \pi/2)$	$v^2 = u^3 - u^2 - 2u$	1	$\{0, \pm 1\}$	5
$(\pi/6, \pi/3)$	$v^2 = u^3 + (\sqrt{3} - 1)u^2 - u + (-\sqrt{3} + 1)$	1	$\{0\}$	7
$(\pi/5, \pi/2)$	$v^2 = u^3 - u^2 + 1/2(\sqrt{5} - 7)u + 1/2(\sqrt{5} - 3)$	1	$\{0\}$	13
$(\pi/5, \pi/3)$	$v^2 = u^3 + 1/2(\sqrt{5} - 1)u^2 + 1/2(\sqrt{5} - 5)u - 1$	1	$\{0, 1\}$	13
$(\pi/5, 2\pi/5)$	$v^2 = u^3 - 2u - 1$	1	$\{0\}$	7
$(\pi/5, 4\pi/5)$	$v^2 = u^3 + 1/2(-\sqrt{5} + 1)u^2 - 4u + (2\sqrt{5} - 2)$	0	$\{0\}$	-

In case of $(\alpha, \beta) = (\pi/5, \pi/3)$ we get the following family of triangles given by the length of the sides

$$(x, y, z_\alpha) = \left(t, t, \frac{-1 + \sqrt{5}}{2}t\right) \text{ and } (x, y, z_\beta) = (t, t, t),$$

where $t \in \mathbb{N}$.

REFERENCES

- [1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [2] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.
- [3] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.
- [4] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, New York, NY, USA, 1992.
- [5] I. Gaál, I. Járás, and F. Luca. A remark on prime divisors of lengths of sides of Heron triangles. *Experiment. Math.*, 12(3):303–310, 2003.
- [6] Richard K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, second edition, 1994. Unsolved Problems in Intuitive Mathematics, I.
- [7] H. Harborth, A. Kemnitz, and N. Robbins. Non-existence of Fibonacci triangles. *Congr. Numer.*, 114:29–31, 1996. Twenty-fifth Manitoba Conference on Combinatorial Mathematics and Computing (Winnipeg, MB, 1995).
- [8] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.
- [9] N. Petulante and I. Kaja. How to generate all integral triangles containing a given angle. *Int. J. Math. Math. Sci.*, 24(8):569–572, 2000.
- [10] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2):323–334, 1983.

MATHEMATICAL INSTITUTE
UNIVERSITY OF DEBRECEN
P.O.BOX 12
4010 DEBRECEN
HUNGARY
E-mail address: `tengely@math.klte.hu`