Algebraic Geometry

Vanya Cheltsov

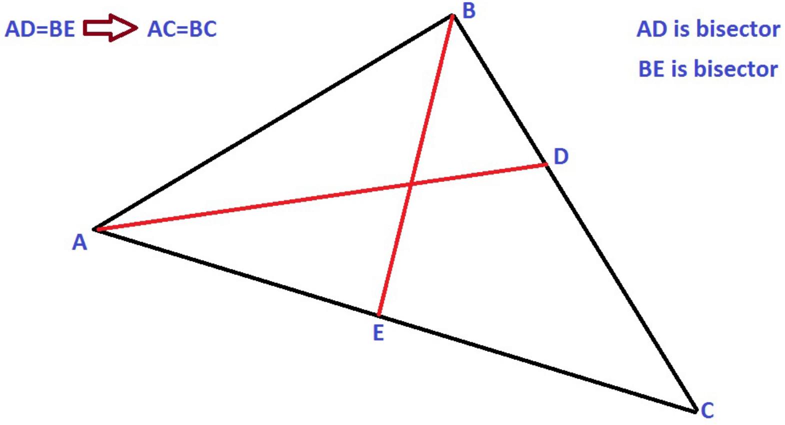
4th February 2019

Lecture 7: Sharygin triangles and elliptic curves

Steiner–Lehmus theorem

Theorem

Every triangle with two angle bisectors of equal lengths is isosceles.



Steiner–Lehmus theorem: the proof

Let ABC be a triangle in $\mathbb{R}^2$.

- Denote by x the length of the side AC.
- Denote by y the length of the side BC.
- Denote by z the length of the side AB.

Let AD be the bisector of the angle $\angle CAB$. Then

$$AD = \sqrt{xz - \frac{xzy^2}{(x+z)^2}}.$$

Let BE be the bisector of the angle $\angle ABC$. Then

$$BE = \sqrt{yz - \frac{yzx^2}{(y+z)^2}}.$$

Thus, if $AD = BE$, then

$$x(x+z)^2(y+z)^2 - xy^2(y+z)^2 - y(x+z)^2(y+z)^2 + yx^2(x+z)^2 = 0.$$

Dividing this polynomial by $x - y$, we get

$$x^3y + 2x^2y^2 + 4x^2yz + x^2z^2 + xy^3 + 4xy^2z + 5xyz^2 + 2xz^3 + y^2z^2 + 2yz^3 + z^4.$$

Problems in Plane Geometry by Igor Sharygin

This book contains about 498 problems in Plane Geometry.

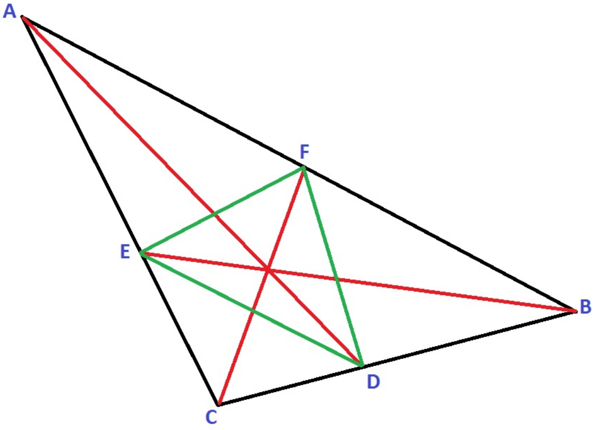
- 143 standard problems.
- 293 difficult problems.
- 62 additional problems.

Additional problem №58

Let ABC be a triangle in $\mathbb{R}^2$.
Let AD, BE, CF be its angle bisectors.

Question

If DEF is isosceles triangle, can ABC be not non-isosceles?



Regular heptagon

Algebra versus Geometry

- Let ABC be a triangle in $\mathbb{R}^2$.
- Let AD be the bisector of the angle $\angle CAB$.
- Let BE be the bisector of the angle $\angle ABC$.
- Let CF be the bisector of the angle $\angle ACB$.

Definition

ABC is Sharygin triangle if DEF is isosceles and ABC is not.

- Let $x = AC$. Let $y = BC$. Let $z = AB$. Let

  $$f(x,y,z) = x^3+x^2y+xy^2+y^2+z(y^2+xy+x^2)-z^2(x+y)-z^3.$$

- Then $DF - EF$ is equal to

  $$(x-y)\frac{xyz}{(x+y)(x+z)^2(y+z)^2}f(x,y,z).$$

Corollary

ABC is Sharygin triangle $\iff$ $f(x,y,z)=0$ *and* $x \neq y$.

Here we assume that DEF is isosceles $\iff$ $DF = EF$.

Weierstrass form

Let $\mathcal{E}$ be the cubic curve in $\mathbb{P}^2_{\mathbb{C}}$ that is given by

$$x^3 + x^2y + xy^2 + y^2 + z(y^2 + xy + x^2) - z^2(x + y) - z^3 = 0.$$

Sharygin triangle are points $[x : y : z] \in \mathcal{E}(\mathbb{R})$ such that $x \neq y$ and

$$\begin{cases} 0 < x < y + z, \\ 0 < y < x + z, \\ 0 < z < y + z. \end{cases}$$

- If $[x : y : z] \in \mathcal{E}$ and $x = y$, then

$$[x : y : z] = [1 \pm \sqrt{17} : 1 \pm \sqrt{17} : 8]$$

  or $[x : y : z] = [-1 : -1 : 1]$.
- The point $[1 : -1 : 0]$ is an inflection point of the curve $\mathcal{E}$.
- There is a projective transformation that maps $\mathcal{E}$ to

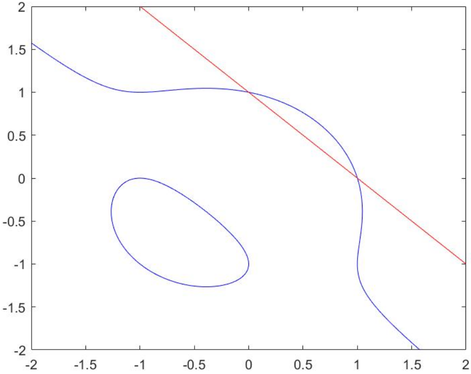
$$zy^2 = x^3 + 5x^2z + 32xz^2.$$

Plotting the cubic curve in Maple

- Let U_z be the subset in $\mathbb{P}^2_{\mathbb{C}}$ given by $z \neq 0$.
- Identify $U_z = \mathbb{C}^2$ with coordinates $\overline{x} = \frac{x}{z}$ and $\overline{y} = \frac{y}{z}$.

Then $\mathcal{E} \cap U_z$ in $\mathbb{C}^2$ is given by

$$\overline{x}^3 + \overline{x}^2\overline{y} + \overline{xy}^2 + \overline{y}^2 + \overline{y}^2 + \overline{xy} + \overline{x}^2 - \overline{x} - \overline{y} - 1 = 0.$$



Integer Sharygin triangles

- We explicitly described all Sharygin triangles.
- The additional problem №58 is completely solved.

Question

Are there Sharygin triangles with integer sides?

Lemma

Yes.

Proof.

Computer search gives one Sharygin triangle with integer sides:

$$\left[1481089 : 18800081 : 19214131\right]$$

$\square$

Question

How many Sharygin triangles with integer sides?

The answer to this question is too complicated for computer.

Group structure

- Let $\mathcal{E}$ be the cubic curve in $\mathbb{P}^2_{\mathbb{C}}$ given by
$$x^3 + x^2y + xy^2 + y^2 + z(y^2 + xy + x^2) - z^2(x + y) - z^3 = 0.$$
- Equip $\mathcal{E}(\mathbb{Q})$ with $+$ such that $[1 : -1 : 0]$ is zero.

The curve $\mathcal{E}$ contains $[1 : 1 : -1]$ and $[1 : 0 : -1]$.

- $2[1 : 1 : -1] = [1 : -1 : 0]$.
- $2[1 : 0 : -1] = [0 : 1 : 1]$.
- $4[1 : 0 : -1] = [25 : -32 : 17]$.

Computing $n[1 : 0 : -1]$ and $n[1 : 0 : -1]+[1 : 1 : -1]$, we get
$$9\big[1 : 0 : -1\big]+\big[1 : 1 : -1\big] = \Big[1481089 : 18800081 : 19214131\Big]$$
and $16\big[1 : 0 : -1\big]$ is a Sharygin triangle with integer sides:
$$\Big[30136153344990045883760 0 : 49105016933436320224063 : 31662903325350128110280 7\Big].$$

Cubic curves over $\mathbb{Q}$

- Let $\mathcal{E}$ be a smooth cubic curve in $\mathbb{P}^2_{\mathbb{C}}$.
- Suppose that $\mathcal{E}$ is defined over $\mathbb{Q}$.
- Suppose that $\mathcal{E}(\mathbb{Q})$ contains a point O.

Equip $\mathcal{E}(\mathbb{Q})$ with $+$ such that O is zero.

Theorem (Mordell, 1922)

The group $\mathcal{E}(\mathbb{Q})$ is a finitely generated abelian group.

Thus, we have

$$\mathcal{E}(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathcal{E}(\mathbb{Q})_{tors},$$

where $\mathcal{E}(\mathbb{Q})_{tors}$ is a finite abelian group.

- The number r is known as the rank of the curve $\mathcal{E}$.
- A folklore conjecture says that r can be arbitrary large.

Theorem (Mazur, 1975)

The group $\mathcal{E}(\mathbb{Q})_{tors}$ is one of the following groups:

- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *for* $m \in \{2, 4, 6, 8\}$,
- $\mathbb{Z}/n\mathbb{Z}$ *for* $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$.

Infinitely many integer Sharygin triangles

- Let $\mathcal{E}$ be the cubic curve in $\mathbb{P}^2_{\mathbb{C}}$ given by
$$x^3 + x^2y + xy^2 + y^2 + z(y^2 + xy + x^2) - z^2(x + y) - z^3 = 0.$$
- Equip $\mathcal{E}(\mathbb{Q})$ with $+$ such that $[1 : -1 : 0]$ is zero.

Then $23\big[1 : 0 : -1\big] + [1 : 1 : -1]$ gives another Sharygin triangle:

$$\Big[119361397031607967398713496044789535174585032475535 :$$
$$: 109775670610677902190285796706340213216430218885103 :$$
$$: 278582753330087324704447274124548850091419264820 9\Big].$$

The next two are $30\big[1 : 0 : -1\big]$ and $37\big[1 : 0 : -1\big] + [1 : 1 : -1]$.

Theorem

The order of the point $[1 : 0 : -1]$ is infinite.

Corollary

There are infinitely many Sharygin triangles with integer sides.

- One can show that the group $\mathcal{E}(\mathbb{Q})$ is $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

MAGMA calculator

Using the following script:

```
P2<x,y,z>:=ProjectiveSpace(Rationals(),2);
C:=Curve(P2,x^3+x^2*y+x*y^2+y^3+x^2*z+
            x*y*z+y^2*z-x*z^2-y*z^2-z^3);
O:= C![1,-1,0];
E:= EllipticCurve(C,O);
TorsionSubgroup(E), Rank(E);
```

we obtain

```
Abelian Group isomorphic to Z/2
Defined on 1 generator
Relations:
    2*$.1 = 0
1 true
```

The table

O	$[1 : -1 : 0]$
Q	$[-1 : -1 : 1]$
P	$[1 : 0 : -1]$
$P + Q$	$[1 : -1 : 1]$
$2P$	$[0 : 1 : 1]$
$2P + Q$	$[1 : 3 : -5]$
$3P$	$[1 : 5 : -4]$
$3P + Q$	$[-9 : 7 : 5]$
$4P$	$[25 : -32 : 17]$
$4P + Q$	$[49 : 11 : -39]$
$5P$	$[128 : 37 : -205]$
$5P + Q$	$[121 : -9 : 119]$
$6P$	$[-1369 : 1425 : 1424]$
$6P + Q$	$[3 : 4067 : -4147]$
$7P$	$[16245 : 17536 : -16909]$
$7P + Q$	$[-48223 : 47311 : 1825]$
$8P$	$[600608 : -622895 : 600153]$
$8P + Q$	$[1681691 : 1217 : -1650455]$
$9P$	$[7659925 : 20017089 : -34783204]$

Nagell-Lutz theorem

Let $\mathcal{C}$ be a smooth cubic in $\mathbb{P}^2_{\mathbb{C}}$ given by

$$zy^2 = x^3 + ax^2z + bxz^2 + cz^3,$$

where a, b and c are some integers. Let

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

- Then D is said to be the discriminant of the curve $\mathcal{C}$.

Equip $\mathcal{C}$ with a group structure with identity $[0 : 1 : 0]$.

Theorem (Nagell, Lutz)

Let x and y be rational numbers such that

$$y^2 = x^3 + ax^2 + bx + c.$$

Suppose that $[x : y : 1]$ is a point of finite order in $\mathcal{C}$. Then

- *both x and y are integer,*
- *if $y = 0$, then $[x : 0 : 1]$ has order 2,*
- *if $y \neq 0$, then y^2 divides D.*

The poster

Sharygin Triangles and Cubic Curves

Tom Adams, Kate Brady, Michael Cairney, Ivan Cheltsov

FACETS of Mathematics 2017

School of Mathematics

A Bit of History

Igor Fedorovich Sharygin, a Russian mathematician, was best known for his contributions to education of geometry. Sharygin was a talented problem writer and wrote exercises for high school students.
However, in relation to his eponymous triangle, Sharygin's most relevant work is the book 'Problems In Geometry, Plane Geometry' [2]. In this book, Sharygin proposed the problem from which his famous triangle was born.

What is a Sharygin Triangle?

A Sharygin Triangle is a triangle that is itself scalene, but has an isosceles bisectral triangle [1]. An example of one such triangle is shown in Figure 1.

Figure 1:

Integer Solutions?

We can easily find integer solutions to (★) (see right hand side of poster), if these are not necessarily positive. The first few that we find are

$$[1:-1:0], [1:1:-1], [1:0:-1], [0:1:1],$$
$$[1:3:-5], [1:5:-4], [3:1:-5], [5:1:-4],$$
$$[-1:1:1], [0:-1:1], [7:-9:5], [-32:25:17].$$

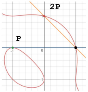
Note that $[1:-1:0]$ is an inflection point of $\mathcal{C}$ (★). The case where $|x|, |y|, |z| < 10000$ is harder to compute. On top of that, no natural triples (which would give a triangle) yet appear in this case . Because of this, we see that using brute force to find our triples will be very hard, even with a machine.
There is another way!

Addition of Points on the Cubic Curve

Equip $\mathcal{C}$ (★) with an operation $+$ such that $O = [1:-1:0]$ is the identity element [3].
Here is an example of this operation: Let $P = [1:0:-1]$. Let us find $2P$:

- The line tangent to $\mathcal{C}$ at P is $y = 0$. This line also crosses $\mathcal{C}$ at $[1:0:1]$.
- The line that passes through O and $[1:0:1]$ also crosses $\mathcal{C}$ at $[0:1:1]$.

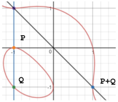
Thus $2P = [0:1:1]$. Here is the visualisation of this procedure:



We can also add two distinct points: Let $P = [1:0:-1]$ and $Q = [1:1:-1]$. Let us find $P+Q$:

- The line that passes through P and Q also crosses $\mathcal{C}$ at $[-1:1:1]$.
- The line that passes through O and $[-1:1:1]$ also crosses $\mathcal{C}$ at $[1:-1:1]$.

Thus $P+Q = [1:-1:1]$.
Here is the visualisation of this procedure:



Sharygin Triangles with Integer Sides

There are infinitely many rational points on the curve $\mathcal{C}$. Let us show why:
We will first apply a projective transformation to $\mathcal{C}$:

$$\begin{cases} \mathbf{x} = -66x - 66y - 87z, \\ \mathbf{y} = 324y - 324x, \\ \mathbf{z} = -2x - 2y - z. \end{cases}$$

This brings our curve to form

$$y^2 z = x^3 - 3267xz^2 + 45630z^3.$$

By the Nagell-Lutz Theorem [3] there are only two rational points of finite order on our transformed curve, and therefore on $\mathcal{C}$. In new coordinates, these are $O = [0:1:0]$ with order 1 and $Q = [15:0:1]$ with order 2 [3]. In old coordinates they are $O = [1:-1:0]$ and $Q = [1:1:-1]$, respectively.
Now we can deduce that, for example the point $P = [1:0:-1]$ has infinite order, and that $O, Q, P, Q+P, 2P, Q+2P, 3P, \ldots$ are all different points. Let us now find some of these points.

point	$\mathcal{C}$
O	$[1:-1:0]$
Q	$[1:1:-1]$
P	$[1:0:-1]$
$Q+P$	$[1:-1:1]$
$2P$	$[0:1:1]$
$Q+2P$	$[1:3:-5]$
$3P$	$[1:5:-4]$
$Q+3P$	$[-9:7:5]$
$4P$	$[25:-32:17]$
$Q+4P$	$[49:11:-39]$
$5P$	$[128:37:-205]$
$Q+5P$	$[121:-9:119]$
$6P$	$[-1369:1425:1424]$
$Q+6P$	$[3:4067:-4147]$
$7P$	$[16245:17536:-16909]$
$Q+7P$	$[-48223:47311:1825]$
$8P$	$[600608:-622895:600153]$
$Q+8P$	$[1681691:1217:-1650455]$
$9P$	$[7659925:20017089:-34783204]$
$Q+9P$	$[1481089:18800081:19214131]$

$Q+9P$ is our first Sharygin triangle with integer coefficients. The next triangle 'happens' at $16P$, then at $Q+23P$ [1]. The higher we go, the longer it takes to compute each one.

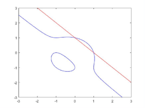
Relation to Cubic Curves

A Sharygin Triangle's sides satisfy the following cubic curve $\mathcal{C}$ in $\mathbb{P}^2$ [1]:

$$x^3 + x^2y + xy^2 + y^3 - z^3 +$$
$$+z(x^2 + xy + y^2) - z^2(x+y) = 0. \quad (★)$$

where $x = AB, y = AC, z = BC$ are the lengths of the sides of the triangle.
As we are in $\mathbb{P}^2$, we can substitute z=1 into (★), for cases where $z \neq 0$, to obtain the curve in $\mathbb{R}^2$ shown in Figure 2:

Figure 2:



Due to the triangle inequality, we are looking for values of (x, y) above the red line. This graph also proves the existence of Sharygin triangles.

References

[1] I. Netay, A. Savvateev, *Sharygin triangles and elliptic curves.* Magadan volume, Bulletin of the Korean Mathematical Society 54 (2017) 1597-1617.

[2] I. F. Sharygin, *Problems in geometry,* Nauka, Moscow, (1982).

[3] J. Silverman, J. Tate, *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer, 2015.