A unique pair of triangles

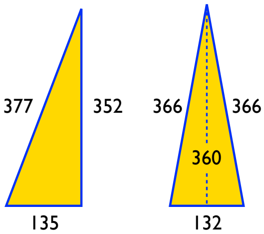
Yoshinosuke Hirakawa and Hideki Matsumura (Keio Univ.)

§1. Main Result

Theorem (H. -Matsumura [2]).
There exists a unique (up to similitude) pair of a right triangle and an isosceles triangle such that

1. all of their sides have integral lengths,
2. they have the same perimeters, and
3. they have the same areas.

The unique pair of triangles are the following:



perimeter
= 377+352+135
= 366+366+132
= 864

area
= 135×352÷2
= 132×360÷2
= 23760

Remark.

1. Every right triangle is characterized by its perimeter and area. Therefore, there exists no incongruent pair of right triangles satisfying 1, 2, and 3.
2. On the other hand, there exist infinitely many incongruent pairs of isosceles triangles satisfying 1, 2, and 3.
3. Moreover, there exist infinitely many pairs of a right triangle and an isosceles triangle satisfying 1 and 2 (resp. 1 and 3).

§2. Hyperelliptic curve

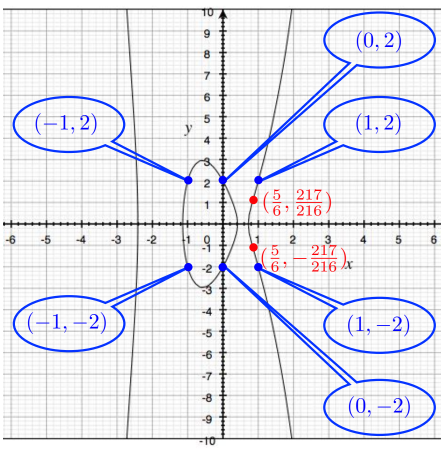
By parameterizing all the pairs of triangles satisfying the three conditions in the above theorem, we can reduce its proof to the following diophantine problem:

Problem.
Determine the set of rational points on the hyperelliptic curve C of genus 2 defined by $y^2 = (x^3 - x + 6)^2 - 32$.

It is easy to check that C has **at least ten** rational points, that is, two points at infinity and $(x, y) = (0, \pm 2), (1, \pm 2), (-1, \pm 2), (5/6, \pm 217/216)$. The first eight points correspond to "collapsed" triangles and the last two points correspond to the above unique pair. Amazingly, **we can prove that**

$$\#C(\mathbb{Q}) \leq 10.$$

This inequality is verified by using the **Chabauty-Coleman method**, which is one of the most sophisticated techniques of modern arithmetic geometry.



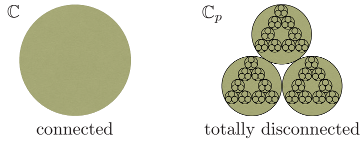
§3. Chabauty-Coleman method

Theorem (Coleman [1]).
Let C be a complete non-singular curve of genus $g > 1$ defined over $\mathbb{Q}$ and J be its jacobian variety. Suppose that C has good reduction at a prime number $p > 2g$ and $r := \operatorname{rank} J(\mathbb{Q}) < g$. Then, we have

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + (2g - 2).$$

Rough idea of the proof of Coleman's theorem:

1. Every closed 1-form on J has a **locally rigid analytic primitive function** because of the "**wobbly topology**" of $\mathbb{C}_p$. Here and after, $\mathbb{C}_p$ denotes the p-adic completion of an algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$. It is a natural p-adic counterpart of the field of complex numbers $\mathbb{C}$, however, it is a **totally disconnected** topological space.



2. We can embed $(C(\mathbb{Q}) \subset)\ J(\mathbb{Q})$ into the r-dimensional subvariety V of $J(\mathbb{C}_p)$ defined by the primitive functions of 1-forms associated with $J(\mathbb{Q}) \subset J(\mathbb{C}_p)$. Then, V cannot contain $C(\mathbb{C}_p)$ because of the assumption $r < g = \dim(J(\mathbb{C}_p))$ and the minimality of J (Chabauty's idea).
3. Reduce the **rigid analytic problem** of estimating the size of $(C(\mathbb{Q}) \subset)\ C(\mathbb{Q}_p) \cap V$ to **algebraic geometry** of the modulo p reduction $C/\mathbb{F}_p$ (cf. $2g - 2 = \deg \Omega^1_{C/\mathbb{F}_p}$).

Remark.
It may be valuable to note a corresponding fact in the case of $g = 1$: If an elliptic curve E defined over $\mathbb{Q}$ has good reduction at an odd prime number p and $\#E(\mathbb{Q}) < \infty$, then the modulo p reduction map induces an injective homomorphism $E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)$ (cf. the Nagell-Lutz theorem).

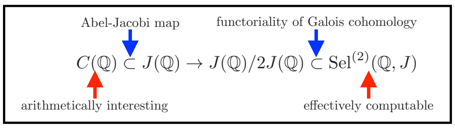
In our case, the hyperelliptic curve C has good reduction at 5, $\#C(\mathbb{F}_5) = 8$ (cf. $(5/6, \pm 217/216) \equiv (0, \pm 2) \pmod 5$), and $\operatorname{rank} J(\mathbb{Q}) \leq 1$. The former two conditions are immediate, however, the last one is not. We can check it by the following **2-descent argument**, which is another of the most sophisticated techniques of modern arithmetic geometry.

§4. 2-descent (cf. Stoll [3])

In the **2-descent argument**, we embed $J(\mathbb{Q})/2J(\mathbb{Q})$ into a certain Galois cohomology group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$, the so called **2-Selmer group** of J. (In fact, we can also use its variants, e.g., $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$.) The dimension of the latter $\mathbb{F}_2$-vector space is **effectively computable (!)** by calculating

1. the **unit group** (i.e., the group of invertible global sections) and
2. the **Picard group** (i.e., the group of invertible sheaves)

of the ring of algebraic integers of $\mathbb{Q}(\alpha | f(\alpha) = 0)$. Here, f denotes a polynomial which defines the branched locus of the double covering $C \to \mathbb{P}^1$, namely, the involved hyperelliptic curve C is defined by $y^2 = f(x)$.



Thank you for your reading!

Reference.
[1] R. F. Coleman, Effective Chabauty, Duke Math. J. 52 (1985), no. 3, 765–770.
[2] Y. Hirakawa and H. Matsumura, A unique pair of triangles, to appear in J. Number Theory (2019).
[3] M. Stoll, Implementing 2-descent for Jacobians of hyperelliptic curves, Acta Arith. 98 (2001), no. 3, 245–277