A unique pair of triangles

David Ang

Wednesday, 12 November 2025

Abstract

This short note recounts a recent result of Hirakawa and Matsumura.

Recall that a triangle is said to be *rational* if its side lengths are all rational, and *integral* if its side lengths are all integral.

Theorem (Hirakawa–Matsumura[1])**.** *Up to similarity, there is a unique pair of a rational right triangle and a rational isosceles triangle with equal perimeter and area, and they are given by* $R_0 := (135, 352, 377)$ *and* $I_0 := (132, 366, 366)$.

By elementary number theory, integral right triangles are parameterised by Pythagorean triples $(2kmn, k(m^2 - n^2), k(m^2 + n^2))$ for some $k, m, n \in \mathbb{N}$. By setting $q := n/m$, this also parameterises rational right triangles by

$$R = (2rq, r(1 - q^2), r(1 + q^2)), \qquad q, r \in \mathbb{Q}.$$

This has perimeter $2r(1 + q)$ and area $r^2 q(1 - q^2)$. On the other hand, every rational isosceles triangle is the union of two identical right triangles, glued along a side adjacent to their right angles. If this adjacent side were parameterised by $2wx$ for some $w, x \in \mathbb{Q}$, then the corresponding rational triangle is given by

$$I = (2w(1 - x^2), w(1 + x^2), w(1 + x^2)), \qquad w, x \in \mathbb{Q}.$$

This has perimeter $4w$ and area $2w^2 x(1 - x^2)$. Otherwise, this adjacent side is necessarily parameterised by $u(1-v^2)$ for some $u, v \in \mathbb{Q}$, and the corresponding rational isosceles triangle is given by

$$(4uv, u(1 + v^2), u(1 + v^2)), \qquad u, v \in \mathbb{Q}.$$

However, this can also be recovered from I by setting $w := u(1 + v)^2/2$ and $x := |(1 - v)/(1 + v)|$, so it suffices to consider pairs of triangles (R, I). By setting $z := r/w$ and equating the perimeters and areas,

$$z(1 + q) = 2, \qquad z^2 q(1 - q^2) = 2x(1 - x^2).$$

The first equation says $q = 2/z - 1$, so substituting it into the second gives $2z^2 - (x^3 - x + 6)z + 4 = 0$. Since $z \in \mathbb{Q}$, the discriminant of $2z^2 - (x^3 - x + 6)z + 4$ as a polynomial in z is necessarily a rational square, or in other words that

$$y^2 = (x^3 - x + 6)^2 - 32, \qquad y \in \mathbb{Q}.$$

[1] **Yoshinosuke Hirakawa and Hideki Matsumura**. A unique pair of triangles. *Journal of Number Theory* 194 (2019), 297–302

This equation cuts out an affine curve, and its non-singular compactification defines a hyperelliptic curve of genus two. In general, a *nice curve* C over a field F will be a smooth proper geometrically integral scheme of dimension one over F, and its *genus* $g_C \in \mathbb{N}$ is the dimension of the first cohomology group of its structure sheaf as a vector space over F. A nice curve C over F is *hyperelliptic* if it admits a degree two morphism to the projective line, so it can be written as the union of the affine curve $y^2 = f(x)$ for some square-free polynomial $f(x) \in F[x]$ of degree $d \in \{2g_C + 1, 2g_C + 2\}$, and the *curve at infinity* $v^2 = u^{2g_C+2} f(1/u)$ glued along $x = 1/u$ and $y = v/u^{g_C+1}$. By the Riemann–Roch theorem, it turns out that every nice curve of genus two is hyperelliptic.

Now let C be a nice curve over $\mathbb{Q}$ with $g_C > 1$. Via the Abel–Jacobi map, C embeds naturally into its *Jacobian variety* J_C, which is an abelian variety of dimension g_C defined as the moduli space of degree zero divisors on C up to linear equivalence. By the Mordell–Weil theorem, its group of rational points $J_C(\mathbb{Q})$ is finitely generated, so it has a finite *torsion subgroup* T_C and a *rank* $r_C \in \mathbb{N}$ such that $J_C(\mathbb{Q}) \cong T_C \oplus \mathbb{Z}^{r_C}$, so in particular $J_C(\mathbb{Q})/2 \cong T_C[2] \oplus \mathbb{F}_2^{r_C}$. This in turn injects into the 2-Selmer group $S_2(J_C(\mathbb{Q}))$, which is a finite-dimensional vector space over $\mathbb{F}_2$ that is computable in principle.

Let $p \in \mathbb{N}$ be a prime. It turns out that the base change C_p of C to $\mathbb{Q}_p$ has a unique *minimal model* $\mathcal{C}_p$ over $\mathbb{Z}_p$. This is a flat proper regular scheme over $\mathbb{Z}_p$ whose base change to $\mathbb{Q}_p$ is C_p, and it is minimal with respect to the partial ordering induced by morphisms of models over $\mathbb{Z}_p$. Then C is said to have *good reduction* at p if the base change $\widetilde{\mathcal{C}}_p$ of $\mathcal{C}_p$ to $\mathbb{F}_p$ is a nice curve over $\mathbb{F}_p$. If C happens to be cut out by a polynomial over $\mathbb{Z}$, then $\widetilde{\mathcal{C}}_p$ can be obtained from C simply by reducing its coefficients modulo p. For instance, if C is hyperelliptic given by an equation $y^2 = f(x)$ for some $f(x) \in \mathbb{Z}[x]$, then C has good reduction at $p > 2$ precisely if it does not divide the discriminant of $f(x)$.

Mordell conjectured that its set of rational points $C(\mathbb{Q})$ is finite, and this was subsequently proved by Faltings using deep results in algebraic geometry. However, his proof is *ineffective*, in the sense that it does not give a recipe to determine $C(\mathbb{Q})$. Coleman, building upon the work of Chabauty, proved an effective version of Mordell's conjecture under certain assumptions.

Theorem (Chabauty–Coleman[2])**.** *Let C be a nice curve over $\mathbb{Q}$ with $g_C > 1$ and $g_C > r_C$ such that C has good reduction at some prime $p > 2g_C$. Then*

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

The key idea is that $C(\mathbb{Q})$ can be embedded into the compact space $J_{C_p}(\mathbb{Q}_p)$ in two different ways. On one hand, it can be embedded into $J_C(\mathbb{Q})$, whose p-adic closure in $J_{C_p}(\mathbb{Q}_p)$ defines a p-adic submanifold of dimension at most r_C. On the other hand, it can be embedded into $C_p(\mathbb{Q}_p)$, whose inclusion into $J_{C_p}(\mathbb{Q}_p)$ via the Abel–Jacobi map defines a one-dimensional p-adic submanifold. In particular, their intersection in a p-adic manifold of dimension $g_C > r_C$ is expected to be discrete, which was what Chabauty proved, and hence finite.

[2]**Robert Coleman**. Effective Chabauty. *Duke Mathematical Journal* 52 (1985), no. 3, 765–770

Coleman refined this idea by introducing a theory of p-adic integration. Let ω be a non-zero differential form on C that reduces to a non-zero differential form on $\widetilde{\mathcal{C}}_p$. By the theory of Newton polygons, any point $P \in \widetilde{\mathcal{C}}_p(\mathbb{F}_p)$ in $C(\mathbb{Q})$ has at most $1 + \operatorname{ord}_P \omega$ preimages in $C(\mathbb{Q})$ whenever C has good reduction at some prime $p > 2 + \operatorname{ord}_P \omega$, so that by the Riemann–Roch theorem,

$$\#C(\mathbb{Q}) \leq \sum_{P \in \widetilde{\mathcal{C}}_p(\mathbb{F}_p)} (1 + \operatorname{ord}_P \omega) \leq \#\widetilde{\mathcal{C}}_p(\mathbb{F}_p) + (2g_C - 2).$$

The assumption $p > 2 + \operatorname{ord}_P \omega$ then holds precisely because $p > 2g_C$.

Returning to the problem at hand, let C be the hyperelliptic curve over $\mathbb{Q}$ with $g_C = 2$ defined as the union of the affine curve C_0 given by

$$y^2 = f(x) := (x^3 - x + 6)^2 - 32,$$

and the curve at infinity C_∞ given by

$$v^2 = (1 - u + 6u^3)^2 - 32u^6.$$

By setting $u = 0$, there are only two points $\infty_+ := (0, 1)$ and $\infty_- := (0, -1)$ in $C_\infty \setminus C_0$, and there are eight obvious points in C_0 that can be computed by searching in a bounded box, which are tabulated as follows.

(x, y)	R	I	$(\widetilde{x}, \widetilde{y})$
$(0, 2)$	$(0, 2, 2)$	$(2, 1, 1)$	$(0, 2)$
$(0, -2)$	$(2, 0, 2)$	$(2, 1, 1)$	$(0, 3)$
$(1, 2)$	$(0, 2, 2)$	$(0, 2, 2)$	$(1, 2)$
$(1, -2)$	$(2, 0, 2)$	$(0, 2, 2)$	$(1, 3)$
$(-1, 2)$	$(0, 2, 2)$	$(4, 2, 2)$	$(4, 2)$
$(-1, -2)$	$(2, 0, 2)$	$(4, 2, 2)$	$(4, 3)$
$\left(\frac{5}{6}, \frac{217}{216}\right)$	$\left(\frac{5}{8}, \frac{44}{27}, \frac{377}{216}\right)$	$\left(\frac{11}{18}, \frac{61}{36}, \frac{61}{36}\right)$	$(0, 2)$
$\left(\frac{5}{6}, -\frac{217}{216}\right)$	$\left(\frac{44}{27}, \frac{5}{8}, \frac{377}{216}\right)$	$\left(\frac{11}{18}, \frac{61}{36}, \frac{61}{36}\right)$	$(0, 3)$

The first six points do not correspond to well-defined triangles, as in each case R has a side with zero length, while the final two points correspond to triangles similar to $R_0 = (135, 352, 377)$ and $I_0 = (132, 366, 366)$.

Now the discriminant of $f(x)$ computes to be $2^{27} \cdot 47$, so C has good reduction at $5 > 2g_C$. The obvious points in C_0 reduce to six distinct points in the affine curve of $\widetilde{\mathcal{C}}_5$ tabulated above as $(\widetilde{x}, \widetilde{y})$, while $\infty_\pm$ reduce to two distinct points in the curve at infinity of $\widetilde{\mathcal{C}}_5$, and these are all of $\widetilde{\mathcal{C}}_5(\mathbb{F}_5)$. Furthermore, $T_C[2]$ contains a point corresponding to the degree zero divisor

$$[(-1 + \sqrt{2}, 0)] + [(-1 - \sqrt{2}, 0)] - [\infty_1] - [\infty_2],$$

and $S_2(J_C(\mathbb{Q}))$ can be computed[3] to be $\mathbb{F}_2 \oplus \mathbb{F}_2$, so $r_C \leq 2 - 1 < g_C$. In particular, the assumptions of the Chabauty–Coleman theorem hold, so $\#C(\mathbb{Q}) \leq (6 + 2) + (2(2) - 2) = 10$. Thus the ten aforementioned points in $C(\mathbb{Q})$ are complete, which proves the Hirakawa–Matsumura theorem.

[3]**Michael Stoll**, Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arithmetica* 98 (2001), no. 3, 245–277