Appendix 17B. Pythagorean triangles of area 6

We begin with the $(3,4,5)$-triangle, which yields an infinite sequence of Pythagorean triangles of area 6 by Theorem 17.1. Are there any other Pythagorean triangles of area 6? To answer this question we need to determine the Mordell-Weil group $E_6^+(\mathbb{Q})$. By considering the divisors of 12, we know that $\phi(E_6^+(\mathbb{Q}))$ is a subgroup of the group Γ generated (multiplicatively) by $(2,2,1),(2,1,2),(3,3,1),(3,1,3)$, which is itself a subgroup of $\{(a,b,c)\in H : abc=1 \text{ in } H\}$.

We already know several points in $E_6^+(\mathbb{Q})$, and therefore several elements of $\phi(E_6^+(\mathbb{Q}))$: We always have $\phi(\mathcal{O})=(1,1,1)$. The torsion point $(6,0)$ yields $\phi((6,0))=(2,6,3)$. The $(3,4,5)$-triangle yields $P=(12,36)\in E_6^+(\mathbb{Q})$ and $\phi(P)=(6,3,2)$, and so $\phi(P+(6,0))=\phi(P)\phi((6,0))=(3,2,6)$. We claim that

$$\phi(E_6^+(\mathbb{Q}))=\{(1,1,1),(2,6,3),(6,3,2),(3,2,6)\}.$$

To prove this we need to show that the remaining elements of $\Gamma\cong(\mathbb{Z}/2\mathbb{Z})^4$ do not belong to Image(ϕ). Since these are both groups, we need only show that two independent generators of $\Gamma/\langle(2,6,3),(6,3,2)\rangle$ do not belong to Image(ϕ):

If $(2,2,1)\in$ Image(ϕ), then there exist integers m,n,u,v,w with $(m,n)=1$ for which

$$m-6n^2=2u^2,\quad m=2v^2,\quad m+6n^2=w^2.$$

This leads to $2v^2+6n^2=w^2$ and so $w^2\equiv 2v^2 \pmod 3$. However $\left(\frac{2}{3}\right)=-1$ and so 3 divides v and w, and hence n, implying that 3 divides $(m,n)=1$, a contradiction.

If $(2,1,2)\in$ Image(ϕ), then there exist integers m,n,u,v,w with $(m,n)=1$ for which

$$m-6n^2=2u^2,\quad m=v^2,\quad m+6n^2=2w^2.$$

This leads to $v^2+6n^2=2w^2$ and so $v^2\equiv 2w^2 \pmod 3$. However $\left(\frac{2}{3}\right)=-1$ and so 3 divides v and w, and hence n, implying that 3 divides $(m,n)=1$, a contradiction.

This establishes the claim, and so since $\phi(E_6^+(\mathbb{Q}))$ includes the image of the torsion point $(6,0)$ we deduce that $E_6^+(\mathbb{Q})$, and so $E_6(\mathbb{Q})$, has rank 1, the infinite part generated by P. Finally $E_6(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}$.

Therefore all of the Pythagorean triangles of area 6 are generated by $nP = (x_n, y_n)$, $n \geq 1$, taking $t = x_n/6$ and $g = 36/|y_n|$.

Integer points

In appendix 6C we need all of the $(x,y) \in E_6(\mathbb{Z})$ with x divisible by 6. The values $t = 2$, 3, and 49 given there correspond to the points $(12, \pm 36)$, $(18, \pm 72)$, and $(294, \pm 5040) \in E_6(\mathbb{Z})$. These are the only such integer points on $E_6(\mathbb{Z})$, but this is difficult to prove. Siegel's Theorem tells us that $E(\mathbb{Z})$ is always finite but finding all of its elements can be quite a challenge. Bennett [1] determines $E_A(\mathbb{Z})$ whenever $A = p$ or $2p$ for some odd prime p:

There are several "families" of integral points that only occur in very special circumstances. For example, if p can be written as the sum of two fourth powers, say, $p = r^4 + s^4$, then $(-(2rs)^2, \pm 4rs(r^4 - s^4)) \in E_{2p}(\mathbb{Z})$. Or if $p^2 = 2m^2 - 1$ for some integer m, then $(m^2, \pm(m^3 - m)) \in E_p(\mathbb{Z})$. None of these types of special circumstances occur when $p \equiv \pm 3 \pmod 8$. In that case, if $(x,y) \in E_A(\mathbb{Z})$, then either $y = 0$ or we have one of the points

$$(-3, \pm 9), (-2, \pm 8), (6 \cdot 2, \pm 6^2), (6 \cdot 3, \pm 6^2 \cdot 2), (6 \cdot 49, \pm 6^2 \cdot 140) \in E_6(\mathbb{Z}),$$

$$(-4, \pm 6), (5 \cdot 9, \pm 5^2 \cdot 12) \in E_5(\mathbb{Z}),\ (22 \cdot 99, \pm 22^2 \cdot 210) \in E_{22}(\mathbb{Z}),$$

or $(29 \cdot 9801, \pm 29^2 \cdot 180180) \in E_{29}(\mathbb{Z})$.

We observe that A divides x for most of these points $(x,y) \in E_A(\mathbb{Z})$. For such points we can provide a good bound on x, assuming the *abc*-Roth conjecture from section 11.5.

Theorem 17.6. *Assume the abc-Roth conjecture. Fix $\delta > 0$. There exists a constant $c_\delta > 0$ such that if $(x,y) \in E_A(\mathbb{Z})$ with x divisible by squarefree A, then $|x| \leq c_\delta A^{2+\delta}$.*

Proof. Select ϵ such that $(1-2\epsilon)(1+\delta) = 1$. Write $x = AX$ so that $y^2 = x^3 - A^2x = A^3(X^3 - X)$. Therefore A^2 divides y as A is squarefree, and so $X^3 - X = AY^2$ where $y = A^2Y$. We now apply the *abc*-Roth conjecture with $F(u,v) = uv(u^2 - v^2)$, so that $F(-1, X) = AY^2$, which yields

$$\kappa_{F,\epsilon}|X|^{2-\epsilon} \leq \prod_{p|AY} p \leq A|Y| = (A \cdot AY^2)^{1/2} < (AX^3)^{1/2}.$$

We deduce that $|X| \leq c_\delta A^{1+\delta}$ where $c_\delta = \kappa_{F,\epsilon}^{-2-2\delta}$, and the result follows. □

There are many techniques to limit integer points in:

[1] Michael Bennett, *Integral points on congruent number curves*, Int. J. Number theory **9** (2013), 1619–1640.