# Concordant pairs in ratios with rank at least two and the distribution of $\theta$-congruent numbers

By Jerome Tomagan DIMABAYAO

Institute of Mathematics, College of Science, University of the Philippines-Diliman, C.P. Garcia Avenue, U.P. Campus, Diliman, Quezon City 1101, Philippines

(Communicated by Kenji FUKAYA, M.J.A., March 14, 2022)

**Abstract:** Let $k$ and $\ell$ be distinct nonzero integers. We show that in every congruence class modulo an integer $m > 1$, there exist infinitely many integers $n$ such that the Mordell-Weil rank over $\mathbf{Q}$ of the elliptic curve $E(kn, \ell n) : y^2 = x(x + kn)(x + \ell n)$ is at least two. We also find that for sufficiently large $T$, the number of square-free integers $n$ with $|n| \leq T$ for which the elliptic curve $E(kn, \ell n)$ has rank at least two is at least $\mathcal{O}(T^{2/7})$.

**Key words:** Elliptic curve; concordant forms; rank.

**1. Introduction.** Let $M$ and $N$ be nonzero integers. Euler's problem on concordant forms asks whether there are integer solutions $(X, Y, Z, W)$ with $\gcd(X, Y) = 1$ to the system

$$X^2 + MY^2 = Z^2, \quad X^2 + NY^2 = W^2. \tag{1.1}$$

Following [7], a pair of integers $(M, N)$ such that $MN \neq 0$ and $M \neq N$ is called a *concordant pair* if the system (1.1) has a solution $(X, Y, Z, W)$ with $XYZ \neq 0$. We note that in studying the system (1.1), we may further assume that $\gcd(M, N)$ is squarefree. It is well known [10] that $(M, N)$ is a concordant pair if and only if the elliptic curve

$$E(M, N) : y^2 = x^3 + (M + N)x^2 + MNx$$

has a nontrivial rational point of order different from 2. In particular, solutions to (1.1) which correspond to torsion points on $E(M, N)$ have been classified completely ([10], Main Corollary 1).

When $M = -N$, we are reduced to the congruent number problem and an integer $N$ is called a congruent number if (1.1) has a nontrivial solution; equivalently, $N$ is the area of a right triangle with rational sides. Bennett [2] proved the existence of infinitely many congruent numbers in any congruence class modulo an integer $m > 1$. In [9], Johnstone and Spearman proved a similar result where the rank of the associated elliptic curve is at least two.

When $M = (s + r)n$ and $N = (s - r)n$ with relatively prime integers $r$ and $s$ such that $r > |s| \geq 0$, we have the more general $\theta$-congruent number problem, which was considered by Fujiwara [6]. An integer $n$ is said to be a $\theta$-congruent number if there is a triangle with rational sides of angle $\theta$ such that $\cos(\theta) = s/r$ and area $A = n\sqrt{r^2 - s^2}$. Abe, Rajan and Ramaroson [1] proved the existence of infinitely many $\theta$-congruent numbers in congruence classes modulo an integer $m > 1$, represented by an integer $a$ such that $\gcd(a, m)$ is squarefree. They further proved that for sufficiently large $T$, the number of integers in the interval $[1, T]$ that are $\theta$-congruent numbers belonging to the residue class $a \pmod{m}$ is at least $\mathcal{O}(\sqrt{T})$. In the case where $A$ is rational, Davis and Spearman [4] proved the existence of infinitely many $\tau$-congruent numbers in any congruence class modulo an integer $m > 1$. Later, Davis [3] proved a similar result where the rank of the associated elliptic curve is at least two.

In this note, we consider concordant pairs in given ratios. In [7], Im has proved that for a positive integer $m > 1$ and an integer $k$, there are infinitely many concordant pairs $(M, N)$ such that $M, N \equiv k \pmod{m}$. Im [8] subsequently provided a parametrization of infinitely many concordant pairs of the form $(kn, \ell n)$ where $n$ is squarefree and used it to obtain a formula for the density of $\theta$-congruent numbers. In this note, we expand upon the above-mentioned results to concordant pairs $(kn, \ell n)$ such

2010 Mathematics Subject Classification. Primary 11G05; Secondary 11D09, 11D45.

doi: 10.3792/pjaa.98.005

that the Mordell-Weil rank of $E(kn,\ell n)(\mathbf{Q})$ is at least two.

**Theorem 1.1.** *Let $k$ and $\ell$ be distinct nonzero integers and let $m$ be a positive integer. Then*:

(i) *Any congruence class modulo $m$ contains infinitely many integers $n$, inequivalent modulo squares, such that the rank of $E(kn,\ell n)$ is at least two. In particular, there are infinitely many concordant pairs $(M,N)$ with $M\equiv k \pmod m$ and $N\equiv \ell \pmod m$ such that the rank of $E(M,N)$ is at least two.*

(ii) *Moreover, there exist positive real numbers $C_1$ and $C_2$, which depend on $k$ and $\ell$, such that if $T>C_1$, then the number of square-free integers $n$ with $|n|\le T$ for which the elliptic curve $E(kn,\ell n)$ has rank at least two is at least $C_2T^{2/7}$.*

This gives the following consequence for $\theta$-congruent numbers.

**Corollary 1.2.** *Let $0<\theta<\pi$ such that $\cos(\theta)=s/r$ with relatively prime integers $r$ and $s$ such that $r>0$. Let $m$ be an integer with $m>1$. Then*

(i) *Any congruence class modulo $m$ contains infinitely many $\theta$-congruent numbers $n$, inequivalent modulo squares, such that the eliptic curve $E((s+r)n,(s-r)n)$ has rank at least two.*

(ii) *There exist positive real numbers $C_1$ and $C_2$, which depend on $\theta$, such that if $T>C_1$, then the number of square-free $\theta$-congruent numbers $n$ in the interval $[1,T]$ for which the elliptic curve $E((s+r)n,(s-r)n)$ has rank at least two is at least $C_2T^{2/7}$.*

## 2. A parametrization of concordant pairs in ratios.

Henceforth, we fix distinct nonzero integers $k$ and $\ell$. If $d$ is a squarefree rational number, the elliptic curve

$$E(kd,\ell d): y^2=x^3+(k+\ell)dx^2+k\ell d^2x$$

is $\mathbf{Q}$-isomorphic to the elliptic curve

$$E(k,\ell)^d: dy^2=x^3+(k+\ell)x^2+k\ell x,$$

which is the $d$-quadratic twist of $E(k,\ell)$. We eliminate the quadratic term in the right-hand side and clear denominators to obtain the following alternative model of $E(k,\ell)^d$:

$$E_{a,b}^d: dy^2=(x+a)(x+b)(x-(a+b)),$$

where

$$a:=3(2k-\ell) \quad \text{and} \quad b:=3(2\ell-k).$$

Clearly, $a$ and $b$ are distinct and $a/b\notin\{-2,-1/2\}$.

We use a well-known method for constructing infinitely many $d$ such that the Mordell-Weil group of the $d$-quadratic twist $E_{a,b}^d$ has rank at least two. This method is based upon the idea of finding a suitable polynomial $d(t)$ and considering the elliptic curve

$$E_{a,b}^{d(t)}: d(t)y^2=(x+a)(x+b)(x-(a+b))$$

over $\mathbf{Q}(t)$. If $E_{a,b}^{d(t)}(\mathbf{Q}(t))$ has a non-torsion point $P$, then for all but finitely many rational numbers $t_0$, the quadratic twist $E(a,b)^{d(t_0)}$ will have a non-torsion point upon specializing the variable $t$ to $t_0$ ([11], Theorem 11.4 p. 271). The parametrization that we will use is derived from [12]. Put

$$D(t)=t(t+1)(t^2+t+1)f(t)g(t)h(t),$$

where

$$\begin{aligned} f(t)&=(a-b)t+(2a+b),\\ g(t)&=(a+2b)t+(b-a),\\ h(t)&=(2a+b)t+(a+2b). \end{aligned}$$

Then

$$D(t)=3^6d(t),$$

where

$$\text{(2.1)} \qquad \begin{aligned} d(t):=t(t+1)(t^2+t+1)((k-\ell)t+k)\\ \times(\ell t+(\ell-k))(kt+\ell), \end{aligned}$$

and we see that the elliptic curve $E_{a,b}^{D(t)}$ is $\mathbf{Q}(t)$-isomorphic to the elliptic curve $E_{a,b}^{d(t)}$.

**Lemma 2.1.** *Let $t\notin\left\{0,-1,\dfrac{k}{\ell-k},\dfrac{k-\ell}{\ell},-\dfrac{\ell}{k}\right\}$ be a rational number and consider the quadratic twist of $E_{a,b}$ by $d(t)$, where $d(t)$ is as in (2.1). Then $E_{a,b}^{d(t)}(\mathbf{Q})$ has rank greater than or equal to 2, for all but finitely many values of $t$.*

*Proof.* Put

$$P_1:=\left(\frac{((a+b)t^2+2bt-a)}{t^2+t+1},\frac{1}{(t^2+t+1)^2}\right),$$

$$P_2:=\left(\frac{(-bt^2+2at+a+b)}{t^2+t+1},\frac{1}{(t^2+t+1)^2}\right).$$

The proof of Theorem 4 of [12] shows that $P_1$ and $P_2$ are independent points in $E_{a,b}^{D(t)}(\mathbf{Q}(t))$. The conclusion is obtained by specialization. ☐

**3. The proof of the theorem.** We prove statement (i) of Theorem 1.1. Suppose $e$ and $m$ are integers with $m > 1$. Define the set $S$ by

$$S = \{s \in \mathbf{Z} \mid s \equiv e \pmod{m}\}.$$

Put $c = k\ell(\ell - k)$ and let $s \in S$. For $x = 1, 2, \ldots$, define $n := \dfrac{d(scx^2m^2)}{c^2x^2m^2}$. That is,

$$n = s(scx^2m^2 + 1)\alpha\beta\gamma\delta, \tag{3.1}$$

where

$$\begin{aligned}
\alpha &= s\ell(\ell - k)^2x^2m^2 + 1,\\
\beta &= sk\ell^2x^2m^2 + 1,\\
\gamma &= s(\ell - k)k^2x^2m^2 + 1, \text{ and}\\
\delta &= s^2c^2x^4m^4 + scx^2m^2 + 1.
\end{aligned}$$

By considering all the possibilities of the signs of $k$ and $\ell$, we notice that $n > 0$ if and only if $s > 0$. By Lemma 2.1, we know that $E(a,b)^n(\mathbf{Q})$ has rank at least two with at most finitely many exceptions. Moreover, we have

$$n \equiv e \pmod{m}.$$

It remains to verify that infinitely many of these integers $n$ are inequivalent modulo $(\mathbf{Q}^\times)^2$. Indeed, if not, then we can find a finite set of nonzero rational numbers, say $\{n_i : i = 1, \ldots, g\}$ which are inequivalent modulo $(\mathbf{Q}^\times)^2$, such that for each $x$ in (3.1), we have

$$\frac{d(scx^2m^2)}{c^2x^2m^2} = n_iy^2, \tag{3.2}$$

with rational numbers $y$ and $n_i$ that depend on $x$. Note that for each $i = 1, \ldots, g$, Eq. (3.2) defines a hyperelliptic curve

$$C_i : n_iY^2 = \frac{d(scX^2m^2)}{c^2X^2m^2} \tag{3.3}$$

of genus 5. The infinitely many distinct values of $x$ that we took give infinitely many distinct rational points on the set $\{C_i : i = 1, \ldots, g\}$. On the other hand, a theorem of Faltings [5] implies that each $C_i$ has only finitely many rational points. We arrive at a contradiction. This completes the proof of (i).

To prove statement (ii), we consider the binary form $F(X,Y) = Y^7d(X/Y)$ of degree 7. We know that $F$ has nonzero discriminant since the polynomial $d(t)$ has distinct roots. The largest degree of an irreducible factor of $F$ is 2, which is less than 5. Thus, the hypotheses of Theorem 1 of [12] are satisfied, giving the desired result. This concludes the proof of Theorem 1.1.

## References

[1] T. Abe, A. Rajan and F. Ramaroson, A few remarks on congruent numbers, Rocky Mountain J. Math. **39** (2009), no. 4, 1083–1088.
[2] M. A. Bennett, Lucas' square pyramid problem revisited, Acta Arith. **105** (2002), no. 4, 341–347.
[3] C. T. Davis, On the distribution of rank two $\tau$-congruent numbers, Proc. Japan Acad. Ser. A Math. Sci. **93** (2017), no. 5, 37–40.
[4] C. T. Davis and B. K. Spearman, On the distribution of $\tau$-congruent numbers, Proc. Japan Acad. Ser. A Math. Sci. **91** (2015), no. 7, 101–103.
[5] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), no. 3, 349–366.
[6] M. Fujiwara, $\theta$-congruent numbers, in *Number theory* (*Eger, 1996*), 235–241, de Gruyter, Berlin, 1998.
[7] B.-H. Im, Concordant numbers within arithmetic progressions and elliptic curves, Proc. Amer. Math. Soc. **141** (2013), no. 3, 791–800.
[8] B.-H. Im, Elliptic curves and the density of $\theta$-congruent numbers and concordant pairs in ratios, J. Pure Appl. Algebra **218** (2014), no. 1, 18–26.
[9] J. A. Johnstone and B. K. Spearman, On the distribution of congruent numbers, Proc. Japan Acad. Ser. A Math. Sci. **86** (2010), no. 5, 89–90.
[10] K. Ono, Euler's concordant forms, Acta Arith. **78** (1996), no. 2, 101–123.
[11] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151, Springer-Verlag, New York, 1994.
[12] C. L. Stewart and J. Top, On ranks of twists of elliptic curves and power-free values of binary forms, J. Amer. Math. Soc. **8** (1995), no. 4, 943–973.