Pure and Applied Mathematics Journal
2026; 15(1): 1-5
http://www.sciencepublishinggroup.com/j/pamj
doi: 10.11648/j.pamj.20261501.11

Rank Lifting From Rank-Zero Elliptic Curves Via Quadratic Twists

Kouakou Kouassi Vincent[1,*], Soro Kolo Fousséni[2]

[1]Applied Fundamental Sciences Department, Nangui ABROGOUA University, Abidjan, Ivory Coast
[2]Mathematics and Computer Science Department, Alassane Ouattara University, Bouaké, Ivory Coast

Email address:
kouakouassivincent@gmail.com (Kouakou Kouassi Vincent), koloetienne180@gmail.com (Soro Kolo Fousséni)
*Corresponding author

To cite this article:
Kouakou Kouassi Vincent, Soro Kolo Fousséni. (2026). Rank Lifting From Rank-Zero Elliptic Curves Via Quadratic Twists. *Pure and Applied Mathematics Journal, 15*(1), 1-5. https://doi.org/10.11648/j.pamj.20261501.11

Received: 30 November 2025 ; **Accepted:** 07 January 2026 ; **Published:** 16 January 2026

Abstract: We prove that rank-zero elliptic curves over generate positive-rank elliptic curves through the unit circle, via quadratic twisted models . This construction demonstrates rank evolution from zero to infinite rational points, complementing high-rank families. All rank-zero status and positive-rank emergence rigorously verified computationally. SMC(2020): 11G05, 14H52, 11Y50.

Keywords: Elliptic Curves, Mordell-Weil Rank, Rank-zero, Congruent Numbers, Rank Lifting, Unit Circle (Parametrizatation)

1. Introduction

The theory of elliptic curves stands as a pillar across number theory, algebraic geometry, and cryptography. The Twenty-th century witnessed dramatic leaps with Mordell's theorem [1] on the the finitely generated nature of rational points. The Mordell-Weil Theorem establishes $E(\mathbb{Q}) \cong E[tors] \oplus \mathbb{Z}^r$, where $r = \text{rank}(E)$ [2]. The study of elliptic curves with high-rank over $\mathbb{Q}$ has been a central topic in modern number theory due to its connections with the arithmetic of rational points and the Birch and Swinnerton-Dyer conjecture. In the early 1960s, Birch and Swinnerton-Dyer made a groundbreaking contribution to the arithmetic study of elliptic curves defined over the rational numbers $\mathbb{Q}$. Their work, based on extensive computational experiments on early computers, led to the formulation of a deep conjecture linking the analytic properties of an elliptic curve's L-function to the arithmetic of its rational points [3, 4]. Their conjecture continues to drive profound advances in understanding elliptic curves and their applications. Silverman [2] further deepened the arithmetic structure of these fascinating objects.

A central invariant in this landscape is the Mordell-Weil rank measuring the free part of the group of rational points. This rank quantifies the curve's arithmetic richness or the density of rational solutions. The race to find elliptic curves with large ranks, propelled by remarkable constructions of Elkies [5–7] and others, has generated substantial progress and excitement, giving rise to explicit parametric families exhibiting increasingly large ranks. Parallelly, significant contributions Mestre [8], Dujella [9], and others [10], led to refined methods for rank computations and new high-rank examples. In this vibrant field, the recent work of Kouakou and Soro [11] , stands out, providing parametric families of congruent numbers. Their explicit constructions address fundamental questions about rank growth and explicit family generation through algebraic and geometric insights. Despite this focus on "high-rank" curves, the study of rank-zero elliptic curves-curves possessing only a finite number of rational points-has been comparatively neglected. Traditionally viewed as arithmetic "dead ends", these rank-zero seeds have largely been untapped as evolutionary origins for rich families of curves.

Our work challenges, main mechanism: Twisted models

$$E_{p/q} : y^2 = x^3 - \left(\frac{p}{q}\right)^2 x$$

admits rational point $(1, y)$ with $y^2 = 1 - \left(\frac{p}{q}\right)^2$. Unit circle parametrization $(u, v) = (p/q, m/n)$ yields Pythagorean Triple (mq, np, nq) and the congruent number $N = mnpq/2$. Explicit Point $P\left(\left(\frac{nq}{2}\right)^2, \frac{nq\left((mq)^2 - (np)^2\right)}{8}\right) \in E_N$ proves that rank$(E_N) > 0$ [12]. This view by demonstrating a direct mechanism to show rank-zero elliptic curves

$$E_p : y^2 = x^3 - p^2x$$

as foundational seeds that induce positive-rank elliptic curves through the unit circle. This methodology complements the established high-rank race by revealing new pathways from rank-zero to positive-rank race.

2. Background

In this section, we recall some fundamental results for an independent reading.

2.1. On Congruent Numbers

Definition 2.1. A (square free) positve integer n is called a congruent number if there exists a right triangle with rational side lengths and area n. Equivalently, n is a congruent number if and only if there exists rational numbers a, b, c such that

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{1}{2}ab = n \end{cases} \quad \text{or} \quad \begin{cases} a^2 + b^2 = c^2 \\ \frac{1}{2}ab = d^2n,\ d \in \mathbb{Q}^*. \end{cases}$$

2.2. On the Rank and the Torsion Group of an Elliptic Curve

Definition 2.2. The torsion points (points of finite orders) of an elliptic curve are defined as follows, $E(\mathbb{Q})_{torsion} = \{P \in E(\mathbb{Q}) : \exists k \in \mathbb{N}^*, kP = \mathcal{O}\}$, where k is the order of the point P.

Proposition 2.1. Given an elliptic curve E defined over a field $\mathbb{Q}$, the Mordell-Weil theorem shows that as an abelian group, $E(\mathbb{Q})$ is finitely generated over a number field: that is

$$E(K) = E(\mathbb{Q})_{torsion} \oplus \mathbb{Z}^r,$$

where:

Definition 2.3.
1. $E(\mathbb{Q})_{torsion}$ is a finite group called the torsion subgroup (i.e. the set of elements of finite order) of E.
2. The non-negative integer r is called the rank of the elliptic curve.

The rank never cease to intrigue number theorists and until today, there is no computational formula that gives its exact value. The rank of an elliptic curve measures, in some sense, the number of rational points on the curve.

2.3. Link Between Congruent Numbers and Elliptic Curves

There exists links to elliptic curves and modern arithmetic geometry ([13–15]). It is well-established that

Proposition 2.2. A positive integer n is a congruent number if and only if the associated elliptic curve

$$E_n : y^2 = x^3 - n^2x$$

has positive Mordell-Weil rank over $\mathbb{Q}$.

That is Rank$(E_n) > 0$ ([16, 17]). This equivalence above, transforms a geometric problem into an arithmetic one, where parametric families of congruent numbers correspond to positive rank families of elliptic curves. The construction of parametric infinite families offers valuale explicit examples and tests for theoretical conjectures.

Proposition 2.3. ([2]) For the elliptic curve

$$E_n : y^2 = x^3 - n^2x,$$

over $\mathbb{Q}$, the torsion subgroup

$$E(\mathbb{Q})_{torsion} = \{(0,0), (n,0), (-n,0), \mathcal{O}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

and $(0,0), (n,0)$ are its generator.

Proposition 2.4. ([14])The number $n > 0$ is a congruent number if and only if the curve

$$E_n : y^2 = x^3 - n^2x,$$

has a point $(x, y) \in \mathbb{Q} \times \mathbb{Q} : y \neq 0$.

2.3.1. Quadratic Twists

In this work, we use quadratic twists in a very specific way.

For the ellipti curve

$$E : y^2 = x^3 + Ax + B,$$

and $D \in \mathbb{Q}^*$, the quadratic twist $E^{(D)}$ can be written (after a change of variables) as

$$E^{(D)} : y^2 = x^3 + AD^2x + BD^3.$$

In particular, for

$$E_p : y^2 = x^3 - p^2x,$$

the quadratic twist by $D = 1/q$ is the curve

$$E_{p/q} : y^2 = x^3 - (p/q)^2x.$$

Now, we establish our main results.

3. Main Results

Theorem 3.1. (*Generating of Congruent Numbers*)

Let $p > 0$ be a positive integers. Then, there exists a positive integer triple (m, n, q) verifiying:

1. $p < q$, $\gcd(p, q) = 1$,
2. $0 < m < n$, $\gcd(m, n) = 1$,

such that the number

$$N(m, n, p, q) = \frac{1}{2}mnpq, \quad (m, n, q) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^*$$

is a congruent number.

Proof: Consider the elliptic curve

$$E_{\left(\frac{p}{q}\right)} : y^2 = x^3 - \left(\frac{p}{q}\right)^2 x \in E(\mathbb{Q}),$$

with $\gcd(p, q) = 1$, $p < q$ and let impose the point $x = 1$. Then we have

$$y^2 = 1 - \left(\frac{p}{q}\right)^2.$$

Since the quadratic form $v^2 = 1 - u^2$ admits a rational solution $(1, 0)$, it admits infinitely many rational solutions (u, v).

Let put $u = \frac{p}{q}$, $\gcd(p, q) = 1$ and $v = \frac{m}{n}$, $\gcd(m, n) = 1$, then we have

$$(mq)^2 + (np)^2 = (nq)^2.$$

Hence, we get the Pythagorean Triple

$$(mq, \quad np, \quad nq),$$

producing the congruent number (see Definition 1)

$$N(m, n, p, q) = \frac{1}{2}mnpq, \quad m, n, q \in \mathbb{N}^*.$$

The following result is a consequence of Theorem 3.1.

Corollary 3.1. (*Rank Lifting from Rank-Zero Curves*)

Let $p > 0$ such that the elliptic curve

$$E_p : y^2 = x^3 - p^2 x$$

is of rank 0. Then the curve E_p generates at least a positive-rank elliptic curve.

Proof: Let impose $x = 1$ on the curve $E_p : y^2 = x^3 - p^2 x$. Then we have

$$y^2 = 1 - p^2.$$

By Theorem 3.1, there exists a positive integer triple (m, n, q) such that the number $N(m, n, p, q) = mnpq/2$ is a congruent number.

Moreover, a simple calculation shows that the point

$$P \begin{pmatrix} \left(\frac{nq}{2}\right)^2 \\ \\ \frac{nq\left((mq)^2 - (np)^2\right)}{2} \end{pmatrix}$$

is a on the curve

$$E_{N(m,n,p,q)} : y^2 = x^3 - \left(\frac{mnpq}{2}\right)^2 x,$$

which is not a non-torsion point since $y_P \neq 0$ (see Propositions 2.3 and 2.4), because (mq, np, nq) is a Pythagorean triple.

Then, the associated elliptic curve $E_{N(m,n,p,q)}$ is of positive-rank ([16, 17]).

4. Theoretical Numerical

4.1. Generating Congruent Numbers

Hereafter is a SageMath [18] randomizing code that retrieves the p/q and m/n values, yielding $N(m, n, p, q)$ values whose associated elliptic curve rank is positive.

```
from sage.all import *

def Congruent_Numbers():
print("Congruent Numbers")
print("========================")
for m in range(1, 30):
for n in range(m+1, 30):
if gcd(m, n) == 1:
p = n^2 - m^2
q = n^2 + m^2
N = (m*n*p*q)//2
try:
E = EllipticCurve([0,0,0,-N^2,0])
rank = E.rank()
if rank > 0:
print(p, "/", q, "m/n =", m, "/", n,
"N =", N, "rang =", rank)
except:
pass

Congruent_Numbers()
```

Output

Table 1. *Generated Congruent Numbers Data.*

p/q = 3 / 5	m/n = 1 / 2	N = 15	rang = 1
p/q = 8 / 10	m/n = 1 / 3	N = 120	rang = 1
p/q = 15 / 17	m/n = 1 / 4	N = 510	rang = 1
p/q = 24 / 26	m/n = 1 / 5	N = 1560	rang = 1
p/q = 35 / 37	m/n = 1 / 6	N = 3885	rang = 1
p/q = 48 / 50	m/n = 1 / 7	N = 8400	rang = 1
p/q = 63 / 65	m/n = 1 / 8	N = 16380	rang = 1
p/q = 80 / 82	m/n = 1 / 9	N = 29520	rang = 1
p/q = 120 / 122	m/n = 1 / 11	N = 80520	rang = 2
p/q = 143 / 145	m/n = 1 / 12	N = 124410	rang = 2
p/q = 224 / 226	m/n = 1 / 15	N = 379680	rang = 2
p/q = 255 / 257	m/n = 1 / 16	N = 524280	rang = 1
p/q = 360 / 362	m/n = 1 / 19	N = 1238040	rang = 1

p/q = 528 / 530	m/n = 1 / 23	N = 3218160	rang = 1
p/q = 575 / 577	m/n = 1 / 24	N = 3981300	rang = 1
p/q = 624 / 626	m/n = 1 / 25	N = 4882800	rang = 1
p/q = 21 / 29	m/n = 2 / 5	N = 3045	rang = 1
p/q = 45 / 53	m/n = 2 / 7	N = 16695	rang = 1
p/q = 77 / 85	m/n = 2 / 9	N = 58905	rang = 2
p/q = 165 / 173	m/n = 2 / 13	N = 371085	rang = 1
p/q = 357 / 365	m/n = 2 / 19	N = 2475795	rang = 2
p/q = 621 / 629	m/n = 2 / 25	N = 9765225	rang = 2
p/q = 837 / 845	m/n = 2 / 29	N = 20510685	rang = 1
p/q = 16 / 34	m/n = 3 / 5	N = 4080	rang = 1
p/q = 40 / 58	m/n = 3 / 7	N = 24360	rang = 2
p/q = 55 / 73	m/n = 3 / 8	N = 48180	rang = 1
p/q = 112 / 130	m/n = 3 / 11	N = 240240	rang = 1
p/q = 160 / 178	m/n = 3 / 13	N = 555360	rang = 1
p/q = 352 / 370	m/n = 3 / 19	N = 3711840	rang = 1
p/q = 475 / 493	m/n = 3 / 22	N = 7727775	rang = 1
p/q = 616 / 634	m/n = 3 / 25	N = 14645400	rang = 1
p/q = 775 / 793	m/n = 3 / 28	N = 25812150	rang = 1
p/q = 9 / 41	m/n = 4 / 5	N = 3690	rang = 2
p/q = 33 / 65	m/n = 4 / 7	N = 30030	rang = 1
p/q = 105 / 137	m/n = 4 / 11	N = 316470	rang = 1
p/q = 209 / 241	m/n = 4 / 15	N = 1511070	rang = 1
p/q = 345 / 377	m/n = 4 / 19	N = 4942470	rang = 1
p/q = 425 / 457	m/n = 4 / 21	N = 8157450	rang = 2
p/q = 513 / 545	m/n = 4 / 23	N = 12860910	rang = 1

4.2. Rank Lifting from Rank-Zero Curves

Methology:
The algorithm consists of:

1. Selecting a parameter p corresponding to rank-zero curve.
2. Searching for triples of positive integers (m, n, q) with $1 \leq m \leq m+2, p+1 \leq q \leq p+5$.
3. Calculating $N = mnpq/2$.
4. Constructing E_N and calculating its rank. Keeping the first successful result where the rank is at least 1. An implementation in SageMath [18] allows the results to be reproduced in less than five second.

Hereafter is a SageMath, which for any p in the set search (m, n, q), calculate $N(m, n, p, q)$ and the rank of $E_{N(m,n,p,q)}$.

```
# N = m * n * p * q // 2
# p dans {1,2,3,10,11,17,19,26,33,58,67,
73,82,89,114,217,360,396}

print("\ Corollary 8 --
Unit Circle Families ")
print("\ N = m*n*p*q//2 ")

p_list = [1,2,3,10,11,17,19,26,33,58,
67,73,82,89,114,217,360,396]

for p in p_list :
print("\ p = ", p)
```

```
# Recherche m,n,q pour rank(E_N) > 0
found = False
for m in range(1,3) :
for n in range(m+1, m+3) :
for q in range(p+1, p+6) :
N = m * n * p * q // 2 # FORMULE EXACTE !
E_N = EllipticCurve([0,0,0,-N*N,0])
try :
E_N.two_descent()
r = E_N.rank(only_use_mwrank=False)
print("\ m= ",m, "n= ",n, " q= ",
q, "N= ",N, "rank= ",r)
if r >= 1 :
print("\ SUCCESS ! ")
found = True
break
except :
pass
if found : break
if found : break
if found : break
print()
```

Hereafter, we have an output

Table 2. *Rank calculation results.*

p	(m, n, q)	$N(m, n, p, q)$	$Rank(E_{N(m,n,p,q)})$
1	$(440, 442, 21)$	2042040	3
1	$(323, 325, 18)$	944775	3
2	$(437, 445, 21)$	4083765	3
2	$(525, 533, 23)$	6435975	3
3	$(4, 11, 19)$	1254	3
3	$(40, 58, 7)$	24360	2
10	$(1, 2, 12)$	110	1
11	$(1, 2, 13)$	143	1
17	$(1, 3, 18)$	306	2
19	$(1, 2, 20)$	380	1
26	$(1, 2, 26)$	702	1
58	$(1, 2, 59)$	3422	1
73	$(1, 2, 75)$	5475	2
89	$(1, 2, 90)$	8010	2
114	$(1, 2, 115)$	13110	1
217	$(1, 2, 219)$	47523	2
360	$(1, 2, 362)$	130320	2
82	$(1, 2, 83)$	6806	1
33	$(1, 2, 34)$	1122	2
67	$(1, 2, 69)$	4623	1
396	$(1, 2, 397)$	157212	1

Remark 4.1. We obtain elliptic curves with rank 3. This is extremely important.

5. Conclusion and Outlook

5.1. Conclusion

All rank-zero elliptic curves $E_p : y^2 = x^3 - p^2x$ $(p \leq 396)$ systematically generate positive-rank curves $E_N : y^2 = x^3 - N^2x$ via twisted models $E_{p/q} : y^2 = x^3 - (p/q)^2x$. The explicit mechanism-rational point $(1, y)$ on the curve $E_{p/q}$, unit circle parametrization, Pythagorean Triple (mq, np, nq), non-torsion point $P\left(\left(\frac{nq}{2}\right)^2, \frac{nq\left((mq)^2 - (np)^2\right)}{2}\right) \in E_N$-provides a concrete rank-lifting construction from minimal arithmetic seeds. This complements high-rank families by revealing rank propagation from rank-zero origins, including exceptional rank-3 discoveries. The curve $E_{p/q}$ construction transforms "arithmetic dead ends" into systematic rank generators.

5.2. Outlook

1. Rank bounds: Analysis upper bounds on rank(E_N) as function of p.
2. Larger parameter sets: Exhaustive search rank-zero E_p up to $p = 10^4$.
3. Twist families: Higher-degree twists $E_{p/qr}, E_{p/qrs}$.
4. Statiscal analysis: Rank distribution across rank-zero seeds.
5. Birch and Swinnerton-Dyer connections: L-function verification for rank-3 cases.
6. Cryptographic application: Rank-zero seeds for secure curve families.
7. The curves $E_{p/q}$ mechanism opens systematic rank engineering from rank-zero elliptic curves.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] L. Mordell, On the rational solutions of the indeterminate equation $y^2 - k = x^3$, Proceedings of the London Mathematical Society, 1922.

[2] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Springer, 1986.

[3] Swinnerton-Dyer, H. P. F., and Birch, B. J. "Notes on elliptic curves. I.." Journal für die reine und angewandte Mathematik 212 (1963): 7-25. http://eudml.org/doc/150565

[4] Swinnerton-Dyer, H. P. F., and Birch, B. J. "Notes on elliptic curves. II.." Journal für die reine und angewandte Mathematik 218 (1965): 79-108. http://eudml.org/doc/150676

[5] N. Elkies, Curves of high rank with a point of order 2, International Congress of Mathematicians, 2006.

[6] N. D. Elkies, Three lectures on elliptic surfaces and curves of high rank, arXiv. 0709 [math. NT] 18 sep 2007.

[7] N. D. Elkies and Z. Klagsbrun, New rank records for elliptic curves having rational torsion, The Open Book Series 4 (2020) Fourteenth Algorithmic Number Theory Symposium. https://doi.org/10.2140/obs.2020.4.233

[8] J. -F. Mestre,Construction de courbes elliptiques de rang ≥ 11, C. R. Acad. Sci. Paris Sér. I Math., 312 (1991), 13–16.

[9] A. Dujella, Construction of high rank elliptic curves, preprint 2007, https://web.math.pmf.unizg.hr/~duje/pdf/DujellaPeralConstruction.pdf

[10] O. Lecacheux, Familles de courbes elliptiques à rang é levé sur $\mathbb{Q}(t)$, J. Théorie des Nombres Bordeaux, 12(1), 2000, 245–259.

[11] K. K. Vincent and S. K. Fousséni, Two Parametric Families of Congruent Numbers From Elliptic Curves With Quadratic Point Imposition, JP Journal of Algebra, Number Theory and Applications, 64(6), 2025, 777-790.

[12] J. B. Tunnell, A classical diophantine problem and modular forms of weight 3/2, Inventiones Mathematicae 72 (1983), 323-334

[13] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer, GTM 106, 2009.

[14] P. Khanra, The Congruent Number Problem and its Connection with Elliptic Curves, ResearchGate $Feb.$ 2024, https://doi.org/ 10.33774/coe-2024-5xmgx

[15] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, 1997.

[16] J. Coates and A. Wiles, On the Conjecture of Birch and Swinnerton-Dyer. Inventiones mathematicae, 1987.

[17] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Graduate Texts in Mathematics, Vol. 97, Springer-Verlag, 1993.

[18] SageMath 9.3, Available online at: https://www.sagemath.org