RAD HAZU. MATEMATIČKE ZNANOSTI
Vol. 29 = 564 (2025): 83-87
DOI: https://doi.org/10.21857/y7v64t4jky

A QUESTION OF ERDŐS ON 3-POWERFUL NUMBERS AND AN ELLIPTIC CURVE ANALOGUE OF THE ANKENY-ARTIN-CHOWLA CONJECTURE

P. G. Walsh

Abstract. We describe how the Mordell-Weil group of rational points on a certain family of elliptic curves give rise to solutions to a conjecture of Erdős on 3-powerful numbers, and state a related conjecture which can be viewed as an elliptic curve analogue of the famous Ankeny-Artin-Chowla conjecture.

1. Introduction

In a series of papers [4],[5],[6], Erdős posed a number of problems concerning powerful numbers. Quite recently, the arithmetic of elliptic curves has been used by Bajpai, Bennett and Chan [2] to prove the existence of infinitely many quadruples of four pairwise coprime powerful numbers in arithmetic progression, thereby answering one of Erdős' problems. In this article we consider a different problem of Erdős. In particular, he asked for solutions to $a + b = c$ in coprime 3-powerful numbers. This was solved by Nitaj [9], and later in a different way by Cohn [3]. Although these solutions were indeed clever, the methods were somewhat ad hoc in nature. We will describe here, in a more systematic manner, how one can produce solutions to Erdős' problem by using the group of rational points on an elliptic curve. It is worth noting here that despite the abundance of coprime solutions to $a + b = c$ in 3-powerful numbers, the *abc* conjecture implies that there are only finitely many triples (a, b, c) consisting of pairwise coprime 4-powerful numbers which satisfy $a + b = c$, and moreover, that no such example is even known to exist (see [7] for details).

Toward this end, it is fairly straightforward to see that a solution to the problem is equivalent to solving the equation

$$ax^3 + by^3 = cz^3$$

2020 *Mathematics Subject Classification.* 11D25, 11G05.
Key words and phrases. Powerful number, diophantine equation, elliptic curve.

in integers for which $rad(a)|x$, $rad(b)|y$, $rad(c)|z$, and $\gcd(ax, by) = 1$. We will make things as simple as possible for ourselves by restricting our attention to the case $a = b = 1$ and $rad(c) = p$, an odd prime, which results in the problem of solving one of

$$x^3 + y^3 = p^\mu z^3 \quad (\mu \in 1, 2)$$

with $(x, y) = 1$ and $p|z$. We will focus primarily on the case $\mu = 1$, as the other case is quite similar. The following result provides a solution to Erdős' problem, however it seems to be merely a first step in this direction.

THEOREM 1.1. *Let p denote an odd prime for which the curve*

$$E : Y^2 = X^3 - 432p^2$$

has positive rank. Then there are infinitely many pairwise coprime integer solutions (x, y, z) to $x^3 + y^3 = p^4 z^3$. Furthermore, if P denotes a generator of infinite order on E, then pairwise coprime integer solutions to $x^3 + y^3 = p^4 z^3$ can be derived from $(3pk)P$ for every integer $k \geq 1$.

To be more explicit we elucidate the above statement. Assume that u, v, d are integers for which $(uv, d) = 1$ and $(X = u/d^2, Y = v/d^3)$ is a point on the curve. Assume further that p divides d. We leave it for the reader to verify that the triple (x, y, z) given by

$$\begin{aligned} x &= num((36pd^3 + v)/6ud), \\ y &= num((36pd^3 - v)/6ud), \\ z &= denom((36pd^3 + v)/6ud) \end{aligned}$$

(all in lowest terms) gives a solution to Erdős' problem.

It is worth remarking at this point that in order to ensure $\gcd(x, y) = 1$ and p divides z, a sufficient condition is for p to divide the integer d defined just above. However, this condition is often not actually necessary. This corresponds to the extra factor of 3 in front of P in the statement of the theorem, which seems to be required only when $p \equiv 1 \pmod 3$.

Adam Logan has pointed out that the 3-Selmer group of E has order 1 for $p \equiv 4, 7, 8 \pmod 9$. Consequently, one would expect the rank of E to be 1 for all of these cases.

2. Proof of Theorem 1.1

We begin by connecting the p-divisibility of d to that of z. The definitions of x, y and z from the previous section imply the existence of a non-zero integer k for which $36pd^3 + v = kx, 36pd^3 - v = ky, 6ud = kz$. Assuming that $p|d$, then because of the fact that u and v are coprime to d, it follows that p does

not divide kx, and therefore cannot be a factor of k. The equation $6ud = kz$ shows that p must be a divisor of z.

We therefore need to pin down the set of points $(X, Y) = (u/d^2, v/d^3)$ on $E : Y^2 = X^3 - 432p^2$ which have the property that p divides d. Let P denote a point of infinite order on E, then regarded as a point on $E(\mathbb{Q}_p)$, the multiple of P having denominator divisible by p is equivalent to the order of P in $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, where $E_0(\mathbb{Q}_p)$ consists of those points whose reduction is non-singular. Since E has additive reduction, this quotient consists of the additive group $\mathbb{Z}/p\mathbb{Z}^+$ of order p times the order of the group of components of the Néron model (see p. 359 of [11]), which in this case is 3. It follows that the point $(3p)P$ has coordinates $(u/d^2, v/d^3)$ satisfying the property that d is divisible by p, which translates into the corresponding value for z in the solution to $x^3+y^3 = pz^3$ being divisible by p, and thus giving integer solutions to Erdős' problem on 3-powerful numbers.

It is worth noting that if m is squarefree, the additive reduction at each prime can be pieced together so that the group structure coming from each prime dividing m can also be glued together to get pairwise coprime integer solutions to $x^3 + y^3 = m^4z^3$ by multiplying a generator by $3m$. A simple example of this phenomenon is given by $m = 35$, in which case a solution to the problem is actually obtained with $35P$, where P is the generator of $E(\mathbb{Q})$, and E is given by $E : Y^2 = X^3-432\cdot35^2$. The corresponding integer solutions (x, y, z) to $x^3 + y^3 = 35^4z^3$ derived from $35P$ have roughly 650 digits, and so we forego displaying them here.

3. An elliptic curve analogue of the Ankeny-Artin-Chowla conjecture

In 1952, Ankeny, Artin and Chowla [1] published a congruence involving various quantities related to a quadratic field and a Bernoulli number, which resulted in a statement which is now referred to as the AAC conjecture. Specifically, the AAC conjecture states that if $p \equiv 1 \pmod 4$ is prime, and if $\epsilon_p = \frac{t+u\sqrt{p}}{2}$ is the fundamental unit of the quadratic field $K = \mathbb{Q}(\sqrt{p})$, then $p \nmid u$. Mordell [8] later conjectured this to be true for $p \equiv 3 \pmod 4$.

An equivalent formulation of this can be stated as follows. If $u = \frac{a+b\sqrt{p}}{2} > 1$ is a unit in the ring of integers of K with $b \equiv 0 \pmod p$, then $u = \epsilon^{kp}$ for some integer k.

This last statement appears to have similarities with the required properties that were required to solve $x^3 + y^3 = p^4z^3$ in pairwise coprime integers.

Let p denote any odd prime, and let $E_{p,2} : Y^2 = X^3 - 432p^2$ and $E_{p,4} : Y^2 = X^3-432p^4$. Let $P = (X, Y)$ denote a generator of one of the curves $E_{p,2}$ or $E_{p,4}$, and $Q = kP = (u/d^2, v/d^3)$ for integers k, u, v, d. We have seen that if the denominator d is divisible by p, then Q gives rise to a solution in pairwise

coprime integers (x, y, z) of $x^3 + y^3 = p^4 z^3$ and $x^3 + y^3 = p^5 z^3$ respectively. Although Theorem 1.1 states that the integer k should be divisible by $3p$, our computations have shown that the desired condition holds very often when k is divisible by p, and thus we state the following as an analogue of AAC for these two families of elliptic curves.

Conjecture 3.1. *EC-AAC*
If P is a generator of $E_{p,2}$ (resp. $E_{p,4}$), and k is a positive integer for which $Q = kP = (u/d^2, v/d^3)$ with $p|d$, then p divides k.

A few cautionary historical remarks are in order. In 1986, when this author learned of the AAC conjecture, the obvious question of whether a similar result holds for composite discriminants led to the immediate discovery that the fundamental units $\frac{t+u\sqrt{d}}{2}$ in $\mathbb{Q}(\sqrt{d})$, with $d = 46$, 430 and 1817, actually have the property that $d|u$. Our observation led to an investigation by Stephens and Williams [12], who produced a longer list of composite values with this property, and very recently, new examples have been found by Reinhart [10], with one of the examples being a prime of the form $4k + 3$, and hence a counterexample to Mordell's extension of AAC. Therefore, one should be extremely wary about the truth of the AAC conjecture. Similarly, the composite value $m = 1349$ has the property that $E_{m,4}$ is generated by a point P having $1349|d$, and presumably a larger search would produce other such curves. We have yet to find a composite integer m for which m divides the integer d arising from a generator of the curve $E_{m,2}$, nor have we found a counterexample to Conjecture 3.1.

Acknowledgements.
The author would like to express gratitude to Noam Elkies, Adam Logan and Joseph Silverman for their extremely helpful discussions.

References

[1] N. C. Ankeny, E. Artin and S. Chowla, *The class-number of real quadratic number fields*, Ann. of Math. (2) **56** (1952), 479–493.
[2] P. Bajpai, M. A. Bennett and T. H. Chan, *Arithmetic progressions in squarefull numbers*, Int. J. Number Theory **20** (2024), 19–45.
[3] J. H. E. Cohn, *A conjecture of Erdős on 3-powerful numbers*, Math. Comp. **67** (1998), 439–440.
[4] P. Erdős, *Consecutive integers*, Eureka Archimedeans J. **38** (1975/76), 3–8.
[5] P. Erdős, *Problems and results on consecutive integers*, Publ. Math. Debrecen **23** (1976), 272–282.
[6] P. Erdős, *Problems and results on number theoretic properties of consecutive integers and related questions*, in: Proceedings of the Fifth Manitoba Conference on Numerical Mathematics, (Univ. Manitoba, Winnipeg, 1975), Congress Numer. XVI, pp. 25–44, Utilitas Math., Winnipeg, 1976.

[7] J.-M. de Koninck and F. Luca, Analytic number theory. Exploring the anatomy of integers, Graduate Studies in Mathematics **134**, American Mathematical Society, Providence, 2012.
[8] L. J. Mordell, *On a Pellian equation conjecture. II*, J. London Math. Soc. **36** (1961), 282–288.
[9] A. Nitaj, *On a conjecture of Erdős on* 3*-powerful numbers*, Bull. London Math. Soc. **27** (1995), 317–318.
[10] A. Reinhart, *A counterexample to the Pellian equation conjecture of Mordell*, Acta Arith. **215** (2024), 85–95.
[11] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.
[12] A. J. Stephens and H. C. Williams, *Some computational results on a problem concerning powerful numbers*, Math. Comp. **50** (1988), 619–632.

Erdősevo pitanje o 3-potentnim brojevima i analogon Ankeny-Artin-Chowline slutnje za eliptičke krivulje

P. G. Walsh

Sažetak. Opisujemo kako Mordell-Weilova grupa racionalnih točaka na određenoj familiji eliptičkih krivulja dovodi do rješenja Erdőseve slutnje o 3-potentnim brojevima i formuliramo povezanu slutnju koja se može promatrati kao analogon poznate Ankeny-Artin-Chowle slutnje za eliptičke krivulje.

P. G. Walsh
Department of Mathematics
University of Ottawa, Canada
E-mail: gwalsh@uottawa.ca

Received: 11.4.2024.
Accepted: 21.5.2024.