Solving problems of Erdös using elliptic curves and an analogue of AAC

Gary Walsh
gwalsh@uottawa.ca

Tutte Institute and
Dept. Math. University of Ottawa
Ottawa, Ontario, Canada

University of Debrecen Online Number Theory Seminar
June 21, 2024

Powerful and k-full Numbers

$n \in \mathbb{Z}^+$ such that $p^2|n$ whenever a prime $p|n$.

i.e. $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ with each p_i prime and $e_i \geq 2$.

Equivalently: $n = ab^2$ for integers a, b with $rad(a)|b$.

Also called *square-full* numbers.

Powerful and k-full Numbers

$n \in \mathbb{Z}^+$ such that $p^2|n$ whenever a prime $p|n$.

i.e. $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ with each p_i prime and $e_i \geq 2$.

Equivalently: $n = ab^2$ for integers a, b with $rad(a)|b$.

Also called *square-full* numbers.

Generalization: n is k-full if $p^k|n$ whenever a prime $p|n$.

Distribution Problems (short intervals, counting, analytic number theoretical)

Additive Problems (sums and differences of powerful numbers)

Connections to the abc conjecture (polynomial values, linear recurrences)

Consecutive Integers (three consecutive powerful numbers?)

Arithmetic progressions of coprime powerful numbers (Erdös asked for four, solved by Bajpai, Bennett and Chan)

Three-term Equations ($x + y = z$ in coprime k-full numbers)

$x + y = z$ in coprime k-full Integers x, y, z

$x + y = z$ in coprime k-full Integers x, y, z

$k = 2$

$x + y = z$ in coprime k-full Integers x, y, z

$k = 2$

Infinitely many solutions: $x^2 + y^2 = z^2$.

$x + y = z$ in coprime k-full Integers x, y, z

$k = 2$

Infinitely many solutions: $x^2 + y^2 = z^2$.

$k = 3$ (posed by Erdös)

$x + y = z$ in coprime k-full Integers x, y, z

$k = 2$

Infinitely many solutions: $x^2 + y^2 = z^2$.

$k = 3$ (posed by Erdös)

Infinitely many solutions (Nitaj, Cohn).

$x + y = z$ in coprime k-full Integers x, y, z

$k = 2$

Infinitely many solutions: $x^2 + y^2 = z^2$.

$k = 3$ (posed by Erdös)

Infinitely many solutions (Nitaj, Cohn).

$k = 4$

$x + y = z$ in coprime k-full Integers x, y, z

$k = 2$

Infinitely many solutions: $x^2 + y^2 = z^2$.

$k = 3$ (posed by Erdös)

Infinitely many solutions (Nitaj, Cohn).

$k = 4$

abc implies only finitely many solutions (Luca-de Koninck).

$x + y = z$ in coprime k-full Integers x, y, z

$k = 2$

Infinitely many solutions: $x^2 + y^2 = z^2$.

$k = 3$ (posed by Erdös)

Infinitely many solutions (Nitaj, Cohn).

$k = 4$

abc implies only finitely many solutions (Luca-de Koninck).

OPEN PROBLEM Find a solution for $k = 4$ or prove that no solution exists.

A new construction to solve the case $k = 3$.

Construct integer solutions to

$$x^3 + y^3 = Nz^3$$

with $rad(N)|z$ and $\gcd(x, y) = 1$.

A new construction to solve the case $k = 3$.

Construct integer solutions to

$$x^3 + y^3 = Nz^3$$

with $rad(N)|z$ and $\gcd(x, y) = 1$.

The curve $x^3 + y^3 = Nz^3$ is birational to $Y^2 = X^3 - 432N^2$ by

$$x = Numer\left(\frac{36N + Y}{6X}\right), y = Numer\left(\frac{36N - Y}{6X}\right),$$

$$z = Denom\left(\frac{36N + Y}{6X}\right).$$

- Start: find an integer N for which the rank is positive.
- We will focus on the case $N = p$ is prime.

Lemma

Let $p > 3$ denote an odd prime, and let

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

If $P = (u/d^2, v/d^3)$ is a point of infinite order on E, with $p|d$, then $(x, y) = 1$ and $p|z$.

i.e. $\quad x^3 + y^3 = p^4(z/p)^3 \quad$ and $\quad \gcd(x, y) = 1.$

POINT: locate points on E which have $p|d$.

```
E:=EllipticCurve([0,-432*49]);
Generators(E);
P:=Generators(E)[1];
for i in [1..10000] do
Q:=i*P;
X:=Q[1];
Y:=Q[2];
d:=Integers()!Floor(Denominator(X)^(1/2));
if d mod 7 eq 0 then
x:=Numerator((36*7+Q[2])/(6*Q[1]));
y:=Numerator((36*7-Q[2])/(6*Q[1]));
z:=Denominator((36*7+Q[2])/(6*Q[1]));
z1:=Integers()!(z/7);
[i,x,y,z1,Gcd(x,y),x^3+y^3-7^4*z1^3];break;
end if;
end for;
```

Cancel　　Submit

```
[ (84 : -756 : 1) ]
true true
[ 21, 56955940266795954130597133248415477948924712042429974970152092787652106296\
1602980334977, -56911242144446914079438646648245772084210267444034499172873618\
6127948731364720791295593, 56569870529305392714755973736657115419456903875459228\
73297440279587838318058950515526, 1, 0 ]
```

A Divisibility Sequence (from multiples of a point)

Let E be an elliptic curve over $\mathbb{Q}$ and $P \in E$ a rational point of infinite order. For $k \geq 1$ define d_k by

$$kP = (u/d_k^2, v/d_k^3) \quad \gcd(u, d_k) = 1.$$

Then the sequence $\{d_k\}$ is a *divisibility sequence*. That is, if $k|l$, then $d_k|d_l$.

A Divisibility Sequence (from multiples of a point)

Let E be an elliptic curve over $\mathbb{Q}$ and $P \in E$ a rational point of infinite order. For $k \geq 1$ define d_k by

$$kP = (u/d_k^2, v/d_k^3) \quad \gcd(u, d_k) = 1.$$

Then the sequence $\{d_k\}$ is a *divisibility sequence*. That is, if $k|l$, then $d_k|d_l$.

Corollary There are infinitely many solutions to Erdös' problem.

Proof. For every $k \geq 1$, the point $Q = (21k)P$ has denominator divisible by 7, giving infinitely many pairwise coprime integer solutions to

$$x^3 + y^3 = 7^4 z^3.$$

```
E:=EllipticCurve([0,-432*49]);
P:=Generators(E)[1];
Q:=42*P;
x:=Numerator((36*7+Q[2])/(6*Q[1]));
y:=Numerator((36*7-Q[2])/(6*Q[1]));
z1:=Denominator((36*7+Q[2])/(6*Q[1]));
z:=Integers()!(z1/7);
Gcd(x,y);
x^3+y^3-7^4*z^3;
x;
y;
z;
```

Cancel

```
1
0
-349129596411643486287421915466340994542177349732209156291625034686096766096525\
1578741546326913048572598868928058785929222099859832311892810174414052759417442\
6500185372826065683911155393134097654689163656112399674898596987660839900849590\
2787723650242130824663870496664076405475685251685151167816231335619974800518017\
7709158764450255994249303579
3513292978984065777446921280126462728890040567352775232582139851847230155401137\
1435386554260083786650900867515627066325933362725215465337943479105705812896076\
7864335189050125213188327798164621546797557161576242265065603073889008286073751\
5558812931315099054190659509140738992838203809702760735198260042380649454107591\
361319496434076096071407579
6959849726009523856451901428704567256435669545753973047566085166693792848073397\
5061929794547076260874883219590115716008744400764792530364804276176920918242651\
4286068323434130484088065194925230935634735871286170888941866587314924677814527\
3074522591005714945145719500418899890763035636148318573785999019167980452043130\
0947817886355442772816980
```

A Variant of Erdós' Problem

$x + y = z$ in coprime k-full numbers with *varying k*

Erdós had remarkable intuition!

The **configuration** $(3, 3, 3)$ has infinitely many solutions 'because'

$$\frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1.$$

Other *such* configurations for this problem:

$$(2, 3, 6), (2, 4, 4)$$

The configuration $(2,3,6)$

$$y^2 = x^3 + pz^6 \quad \text{with} \quad p|z,\ \gcd(x,y) = 1.$$

Find a prime for which $E_p : Y^2 = X^3 + p$ has positive rank, and then find points (X, Y) on E with $Denom(X)$ divisible by p.

The configuration $(2,3,6)$

$$y^2 = x^3 + pz^6 \quad \text{with} \quad p|z,\ \gcd(x,y) = 1.$$

Find a prime for which $E_p : Y^2 = X^3 + p$ has positive rank, and then find points (X, Y) on E with $Denom(X)$ divisible by p.

$E_5 : Y^2 = X^3 + 5$ has rank 1 generated by $(X, Y) = (-1, 2)$.

Let $P = (-1, 2)$ and $kP = (u_k/d_k^2, v_k/d_k^3)$, then

$$5|d_k \quad \text{iff} \quad 5|k.$$

```
p:=5;
E:=EllipticCurve([0,p]);
P:=Generators(E)[1];P;
for i in [1..3] do
Q:=(5*i)*P;
x:=Numerator(Q[1]);
y:=Numerator(Q[2]);
z1:=Integers()!Isqrt(Denominator(Q[1]));
z:=z1/5;
Gcd(x,y);
y^2-x^3-5^7*z^6;
[x,y,z];
print(" ");
end for;
```

Cancel

```
(-1 : -2 : 1)
1
0
[ 176488611599, -74143869240845882, 6421 ]

1
0
[ 970204503045428758752270929324937501564538601,
-3022099581092337504511641307685964689164872787827966440453419954290l,
952155568790942816644 ]

1
0
[ 1661149242006888819335346866931665390917269061924101375628117604617802516731 5\
89110191758503217460943 99, -677283719545010284053159583399080517654063074124630\
295359403456645486947541008802988492869774785456735742456141163244440511271532 0\
820528011448034901648 2, 1868927271373945628243015767096566127931781050856 3 ]
```

The configuration $(2, 4, 4)$

Solve $py^2 = x^4 + z^4$ with $\gcd(x, z) = 1$ and $p|y$.

Work with the curve

$$H : Y^2 = pX^4 + pZ^4, \quad (\textit{want } p^2|Y)$$

where p is any prime which is a sum of two fourth powers. (use the summands to create a *base point* on the hyperelliptic curve, and transform it into a Weierstrass model, and use the structure of the MW group).

The configuration $(2,4,4)$

Solve $py^2 = x^4 + z^4$ with $\gcd(x,z) = 1$ and $p|y$.

Work with the curve

$$H:\; Y^2 = pX^4 + pZ^4, \quad (\textit{want } p^2|Y)$$

where p is any prime which is a sum of two fourth powers. (use the summands to create a *base point* on the hyperelliptic curve, and transform it into a Weierstrass model, and use the structure of the MW group).

$p = 17 = 1^4 + 2^4$ works like a charm!!

```
R<x>:=PolynomialRing(Rationals());b:=17;
h:=HyperellipticCurve(b*x^4+b);h;
e,eto := EllipticCurve(h,h![2,17,1]);e;
MinimalModel(e);Rank(e);#Generators(e);
_,efrom := IsInvertible(eto);

P1:=Generators(e)[1];P2:=Generators(e)[2];P3:=Generators(e)[3];P4:=Generators(e)[4];
for i in [0..0] do for j in [0..0] do for k in [-1..-1] do for l in [-2..-2] do
Q:=efrom(i*P1+j*P2+k*P3+l*P4);q:=Integers()!Q[2];
if q mod 17^2 eq 0 then print(" ");
y1:=Integers()!Q[2];y:=Integers()!(y1/289);x:=Integers()!Q[1];z:=Integers()!Q[3];

[x,y,z];17^3*y^2-x^4-z^4;Gcd(x,z);

end if;end for;end for;end for;end for;
```

Cancel

```
Hyperelliptic Curve defined by y^2 = 17*x^4 + 17 over Rational Field
Elliptic Curve defined by y^2 + 8/17*x*y + 15360/4913*y = x^3 - 784/289*x^2 -
160768/83521*x over Rational Field
Elliptic Curve defined by y^2 = x^3 - 1156*x over Rational Field
2 true
4

[ 427511122, -25071676161582497, 1322049209 ]
0
1
```

Part II. An Elliptic Curve Analogue of the Ankeny-Artin-Chowla Conjecture

Consider the family of curves from earlier

$$y^2 = x^3 - 432p^2 \qquad (p > 3, \ \text{prime}),$$

and assume (for simplicity) that $rank(E) = 1$, and that E has no non-trivial torsion.

Question: For which multiples of the generator does p divide the denominator?

(similar to asking when does $p|U_k$, where $\frac{T_k + U_k\sqrt{p}}{2} = \epsilon_p^k$, where ϵ_p is the fundamental unit in a quadratic field.)

```
for j in [3..20] do
p:=NthPrime(j);
E:=EllipticCurve([0,-432*p^2]);
if Rank(E)*#TorsionSubgroup(E) eq 1 then
P:=Generators(E)[1];
for i in [1..1000] do
Q:=i*P;X:=Q[1];Y:=Q[2];
tell,d:=IsSquare(Denominator(X));
if d mod p eq 0 then
x:=Numerator((36*p+Q[2])/(6*Q[1]));
y:=Numerator((36*p-Q[2])/(6*Q[1]));
z:=Denominator((36*p+Q[2])/(6*Q[1]));
z1:=Integers()!(z/p);
[p,p mod 3,i];break;
end if;
end for;
end if;
end for;
```

Cancel

```
[ 7, 1, 21 ]
[ 13, 1, 39 ]
[ 17, 2, 17 ]
[ 31, 1, 93 ]
[ 43, 1, 129 ]
[ 53, 2, 53 ]
[ 61, 1, 183 ]
[ 67, 1, 201 ]
[ 71, 2, 71 ]
```

Theorem

Let $p > 3$ denote an odd prime. Let E denote the curve

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

Assume that $E_{tor} = \{\mathcal{O}\}$, and $rk(E) = 1$ with generator P.

Let $\mu = \begin{cases} 1 & \text{if } p \equiv 2 \pmod 3 \\ 3 & \text{if } p \equiv 1 \pmod 3. \end{cases}$

Then for every positive integer k, the point $Q = k \cdot (\mu P)$ has denominator divisible by p.

Proof. (Neron) $E(\mathbb{Q}_p)$ has additive type IV reduction $\bmod p$, the order of P in $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ divides $3p$, where $E_0(\mathbb{Q}_p)$ is the set of $\mathbb{Q}_p$-points with non-singular reduction (see Ch.7 and Sect. 15 of Appendix C in Silverman).

The Ankeny-Artin-Chowla Conjecture (AAC)

Let $p \equiv 1 \pmod 4$ denote an odd prime and

$$\epsilon_p = \frac{T + U\sqrt{p}}{2}$$

denote the fundamental unit in $\mathbb{Q}(\sqrt{p})$. Then $p \nmid U$.

The Ankeny-Artin-Chowla Conjecture (AAC)

Let $p \equiv 1 \pmod 4$ denote an odd prime and

$$\epsilon_p = \frac{T + U\sqrt{p}}{2}$$

denote the fundamental unit in $\mathbb{Q}(\sqrt{p})$. Then $p \not| U$.

• False for composite discriminants: $d \in \{46, 430, 1817, \ldots\}$
• Extended to $p \equiv 3 \pmod 4$ by Mordell, but recently shown to be **false** by Andreas Reinhart (2024).
• No theoretical basis, a dubious conjecture.

The Ankeny-Artin-Chowla Conjecture (reformulated)

Let $p \equiv 1 \pmod 4$ denote an odd prime, $k \geq 1$, and

$$\epsilon_p^k = \frac{T_k + U_k\sqrt{p}}{2},$$

where ϵ_p denotes the fundamental unit in $\mathbb{Q}(\sqrt{p})$.

If $p|U_k$, then $p|k$.

Proof. The binomial theorem.

The Ankeny-Artin-Chowla Conjecture (reformulated)

Let $p \equiv 1 \pmod 4$ denote an odd prime, $k \geq 1$, and

$$\epsilon_p^k = \frac{T_k + U_k\sqrt{p}}{2},$$

where ϵ_p denotes the fundamental unit in $\mathbb{Q}(\sqrt{p})$.

If $p|U_k$, then $p|k$.

Proof. The binomial theorem.

Examples:
$\epsilon_3^3 = (2+\sqrt{3})^3 = 26 + 15\sqrt{3} = 26 + 5 \cdot 3\sqrt{3}$
$\epsilon_5^5 = (\frac{1+\sqrt{5}}{2})^5 = \frac{11+5\sqrt{5}}{2}$
$\epsilon_7^7 = (8+3\sqrt{7})^7 = 130576328 + 7050459 \cdot 7\sqrt{7}$
$\epsilon_{46} = 24335 + 3588\sqrt{46} = 24335 + 78 \cdot 46\sqrt{46}$

An Elliptic Curve analogue of AAC for rank 1 curves.

Let $p > 3$ denote an odd prime, Let E denote the curve

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

Assume that $E_{tor} = \{\mathcal{O}\}$, and $rk(E) = 1$ with generator P.

If $k \geq 1$ is a positive integer for which $p | d_k$ (the denominator of kP), then $p | k$.

An Elliptic Curve analogue of AAC for rank 1 curves.

Let $p > 3$ denote an odd prime, Let E denote the curve

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

Assume that $E_{tor} = \{\mathcal{O}\}$, and $rk(E) = 1$ with generator P.

If $k \geq 1$ is a positive integer for which $p|d_k$ (the denominator of kP), then $p|k$.

• **false** for composites: $m = 1349$, $E_{m,4}(\mathbb{Q}) =< P >$ and the denominator of P is divisible by 1349.

An Elliptic Curve analogue of AAC for rank 1 curves.

Let $p > 3$ denote an odd prime, Let E denote the curve

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

Assume that $E_{tor} = \{\mathcal{O}\}$, and $rk(E) = 1$ with generator P.

If $k \geq 1$ is a positive integer for which $p|d_k$ (the denominator of kP), then $p|k$.

• **false** for composites: $m = 1349$, $E_{m,4}(\mathbb{Q}) =< P >$ and the denominator of P is divisible by 1349.
• Finding a counterexample is likely impossible because of the size of the generators. A counterexample p is likely to exist with $p \approx 10^{20}$ (very roughly speaking), and heuristics imply that a generator would have roughly 10^{10} digits.

A more general Elliptic Curve analogue of AAC.

Let $p > 3$ denote an odd prime, Let E denote the curve

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

and assume that E has positive rank and no nontrivial torsion.

Then there is a point $(u/d^2, v/d^3)$ on E for which $\gcd(p, d) = 1$.

Elliptic Wieferich Primes (for singular reductions)

$p > 2$ is a *Wieferich Prime* if $2^{p-1} \equiv 1 \pmod{p^2}$.

Examples: 1093, 3511
(the only known examples up to $1.8 \cdot 10^{19}$)

Elliptic Wieferich Primes (for singular reductions)

$p > 2$ is a *Wieferich Prime* if $2^{p-1} \equiv 1 \pmod{p^2}$.

Examples: 1093, 3511
(the only known examples up to $1.8 \cdot 10^{19}$)

Definition Let $p > 3$ be a prime, $\mu = \mu(p)$ as above, and let E be given by

$$E : y^2 = x^3 - 432p^2.$$

If $P = (u/d_1^2, v/d_1^3) \in E$ with $(p, d_1) = 1$, (non-torsion)

then p is an *Elliptic Wieferich Prime* for (E, P) if

$$Q = (\mu p)P = (u_p/d_{\mu p}^2, v_p/d_{\mu p}^3)$$

satisfies $p^2 | d_{\mu p}$.

Computational Challenge

Find Elliptic Wieferich Primes or AAC counterexamples for curves of the form

$$y^2 = x^3 - 432p^2$$

or curves in other families having singular reduction $\pmod p$.

($E : y^2 = x^3 + k$ with $k = \pm sp^t$, s smooth and $p > c_0(s)$.)

Computational Challenge

Find Elliptic Wieferich Primes or AAC counterexamples for curves of the form

$$y^2 = x^3 - 432p^2$$

or curves in other families having singular reduction $\pmod{p}$.

($E : y^2 = x^3 + k$ with $k = \pm sp^t$, s smooth and $p > c_0(s)$.)

☺ **THANK YOU FOR YOUR ATTENTION** ☺