On the Diophantine equation $X^{2N} + 2^{2L}p^{2M} = Z^5$

Eva Goedhart

Bryn Mawr College

Main Theorem

Theorem (G-)

The equation

$$X^{2N} + 2^{2L}p^{2M} = Z^5$$

has no solution for odd prime p, with X, Z, N, L, $M \in \mathbb{Z}^+$, $N > 1$, and $\gcd(X, Z, 2p) = 1$.

Main Theorem

Theorem (G-)

The equation

$$X^{2N} + 2^{2L}p^{2M} = Z^5$$

has no solution for odd prime p, with X, Z, N, L, $M \in \mathbb{Z}^+$, $N > 1$, and $\gcd(X, Z, 2p) = 1$.

In the proof, I use methods from

- Bennett (2006)
- Bennett & Skinner (2004)

Preliminaries

$$X^{2N} + 2^{2L}p^{2M} = Z^5$$

Preliminaries

$$X^{2N} + 2^{2L}p^{2M} = Z^5$$

We can assume that N is prime.

Preliminaries

$$X^{2N} + 2^{2L} p^{2M} = Z^5$$

We can assume that N is prime.

Lemma (Bennett)

If $a, b, c \in \mathbb{Z} - \{0\}$ *s.t.* $a^2 + b^2 = c^5$ *with* $\gcd(a, b, c) = 1$, *then* $\exists\, u, v \in \mathbb{Z} - \{0\}$ *coprime of opposite parity s.t.*

$$a = u(u^4 - 10u^2v^2 + 5v^4)$$

and

$$b = v(v^4 - 10u^2v^2 + 5u^4).$$

Modular Approach

Let $E/\mathbb{Q}$ be an elliptic curve.

Modular Approach

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime $q \in \mathbb{Z}$, let

$$a_q(E) = (q+1) - |\overline{E}(\mathbb{F}_q)|.$$

Modular Approach

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime $q \in \mathbb{Z}$, let

$$a_q(E) = (q+1) - |\overline{E}(\mathbb{F}_q)|.$$

The trace is bounded by $-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}$.

Modular Approach

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime $q \in \mathbb{Z}$, let

$$a_q(E) = (q+1) - |\overline{E}(\mathbb{F}_q)|.$$

The trace is bounded by $-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}$.

"Arises from", $\sim_n$, is an equivalence relation.

Modular Approach

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime $q \in \mathbb{Z}$, let

$$a_q(E) = (q+1) - |\overline{E}(\mathbb{F}_q)|.$$

The trace is bounded by $-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}$.

"Arises from", $\sim_n$, is an equivalence relation.

Lemma

Let E, F be an elliptic curves over $\mathbb{Q}$ with conductors N, M.

Modular Approach

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime $q \in \mathbb{Z}$, let

$$a_q(E) = (q+1) - |\overline{E}(\mathbb{F}_q)|.$$

The trace is bounded by $-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}$.

"Arises from", $\sim_n$, is an equivalence relation.

Lemma

Let E, F be an elliptic curves over $\mathbb{Q}$ with conductors N, M. If $E \sim_n F$, then $\forall q$, prime,

Modular Approach

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime $q \in \mathbb{Z}$, let

$$a_q(E) = (q+1) - |\overline{E}(\mathbb{F}_q)|.$$

The trace is bounded by $-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}$.

"Arises from", $\sim_n$, is an equivalence relation.

Lemma

Let E, F be an elliptic curves over $\mathbb{Q}$ with conductors N, M. If $E \sim_n F$, then $\forall q$, prime,

- *if $q | NM$, then $a_q(E) \equiv a_q(F) \pmod{n}$, or*

Modular Approach

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime $q \in \mathbb{Z}$, let

$$a_q(E) = (q+1) - |\overline{E}(\mathbb{F}_q)|.$$

The trace is bounded by $-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}$.

"Arises from", $\sim_n$, is an equivalence relation.

Lemma

Let E, F be an elliptic curves over $\mathbb{Q}$ with conductors N, M. If $E \sim_n F$, then $\forall q$, prime,

- *if $q|NM$, then $a_q(E) \equiv a_q(F) \pmod{n}$, or*
- *if $q||N$ and $q \nmid M$, then $a_q(F) \equiv \pm(q+1) \pmod{n}$.*

Theorem (Bennett-Skinner)

For prime $n \geq 7$, $\quad Ax^n + By^n = Cz^2$

Theorem (Bennett-Skinner)

For prime $n \geq 7$, $\quad Ax^n + By^n = Cz^2 \quad$ *(w/ a few conditions)*

Theorem (Bennett-Skinner)

For prime $n \geq 7$, $\quad Ax^n + By^n = Cz^2 \quad$ *(w/ a few conditions) has*

$$E: \quad Y^2 + XY = X^3 + \frac{Cz-1}{4}X^2 + \frac{BCy^n}{64}X.$$

Theorem (Bennett-Skinner)

For prime $n \geq 7$, $\quad Ax^n + By^n = Cz^2 \quad$ *(w/ a few conditions) has*

$$E: \quad Y^2 + XY = X^3 + \frac{Cz-1}{4}X^2 + \frac{BCy^n}{64}X.$$

If $v_2(By^n) \geq 6$, $z \equiv C \pmod 4$, *and* $xy \neq \pm 1$,

Theorem (Bennett-Skinner)

For prime $n \geq 7$, $\quad Ax^n + By^n = Cz^2 \quad$ *(w/ a few conditions) has*

$$E: \quad Y^2 + XY = X^3 + \frac{Cz-1}{4}X^2 + \frac{BCy^n}{64}X.$$

If $v_2(By^n) \geq 6$, $z \equiv C \pmod 4$, and $xy \neq \pm 1$, then E has conductor

$$N' = \begin{cases} 2^{-1}C^2\, rad(ABxy), & \text{if } v_2(By^7) = 6, \\ C^2\, rad(ABxy), & \text{if } v_2(By^7) \geq 7. \end{cases}$$

Theorem (Bennett-Skinner)

For prime $n \geq 7$, $\quad Ax^n + By^n = Cz^2 \quad$ *(w/ a few conditions) has*

$$E: \quad Y^2 + XY = X^3 + \frac{Cz-1}{4}X^2 + \frac{BCy^n}{64}X.$$

If $v_2(By^n) \geq 6$, $z \equiv C \pmod 4$, and $xy \neq \pm 1$, then E has conductor

$$N' = \begin{cases} 2^{-1}C^2\, rad(ABxy), & \text{if } v_2(By^7) = 6, \\ C^2\, rad(ABxy), & \text{if } v_2(By^7) \geq 7. \end{cases}$$

and $E \sim_n f$,

Theorem (Bennett-Skinner)

For prime $n \geq 7$, $\quad Ax^n + By^n = Cz^2 \quad$ *(w/ a few conditions) has*

$$E: \quad Y^2 + XY = X^3 + \frac{Cz-1}{4}X^2 + \frac{BCy^n}{64}X.$$

If $v_2(By^n) \geq 6$, $z \equiv C \pmod 4$, *and* $xy \neq \pm 1$, *then* E *has conductor*

$$N' = \begin{cases} 2^{-1}C^2\, rad(ABxy), & \text{if } v_2(By^7) = 6, \\ C^2\, rad(ABxy), & \text{if } v_2(By^7) \geq 7. \end{cases}$$

and $E \sim_n f$, *for some newform* f *of level*

$$N = \begin{cases} C^2\, rad(AB), & \text{if } v_2(B) \neq 0, 6, \\ 2C^2\, rad(AB), & \text{if } v_2(B) = 0, \\ 2^{-1}C^2\, rad(AB), & \text{if } v_2(B) = 6. \end{cases}$$

Theorem (Bennett-Skinner)

For prime $n \geq 7$, $\quad Ax^n + By^n = Cz^2 \quad$ *(w/ a few conditions) has*

$$E: \quad Y^2 + XY = X^3 + \frac{Cz-1}{4}X^2 + \frac{BCy^n}{64}X.$$

If $v_2(By^n) \geq 6$, $z \equiv C \pmod 4$, and $xy \neq \pm 1$, then E has conductor

$$N' = \begin{cases} 2^{-1}C^2\, rad(ABxy), & \text{if } v_2(By^7) = 6, \\ C^2\, rad(ABxy), & \text{if } v_2(By^7) \geq 7. \end{cases}$$

and $E \sim_n f$, for some newform f of level

$$N = \begin{cases} C^2\, rad(AB), & \text{if } v_2(B) \neq 0, 6, \\ 2C^2\, rad(AB), & \text{if } v_2(B) = 0, \\ 2^{-1}C^2\, rad(AB), & \text{if } v_2(B) = 6. \end{cases}$$

Further, E has nontrivial 2-torsion.

Proof of the Main Theorem

Suppose that $(X, Z, N, L, M) = (x, z, n, \ell, m)$ is a solution to

$$X^{2N} + 2^{2L}p^{2M} = Z^5,$$

Proof of the Main Theorem

Suppose that $(X, Z, N, L, M) = (x, z, n, \ell, m)$ is a solution to

$$X^{2N} + 2^{2L}p^{2M} = Z^5,$$

with $p \geq 3$ and x, z, n, ℓ, $m \in \mathbb{Z}^+$, $n > 1$, and $\gcd(x, z, 2p) = 1$.

Proof of the Main Theorem

Suppose that $(X, Z, N, L, M) = (x, z, n, \ell, m)$ is a solution to

$$X^{2N} + 2^{2L} p^{2M} = Z^5,$$

with $p \geq 3$ and x, z, n, ℓ, $m \in \mathbb{Z}^+$, $n > 1$, and $\gcd(x, z, 2p) = 1$. So

$$x^{2n} + 2^{2\ell} p^{2m} = z^5.$$

Proof of the Main Theorem

Suppose that $(X, Z, N, L, M) = (x, z, n, \ell, m)$ is a solution to

$$X^{2N} + 2^{2L}p^{2M} = Z^5,$$

with $p \geq 3$ and x, z, n, ℓ, $m \in \mathbb{Z}^+$, $n > 1$, and $\gcd(x, z, 2p) = 1$. So

$$x^{2n} + 2^{2\ell}p^{2m} = z^5.$$

Notice that $\gcd(x, 2p) = \gcd(z, 2p) = gcd(x, z) = 1$.

$$x^{2n} + 2^{2\ell} p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

$$x^{2n} + 2^{2\ell} p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$x^{2n} + 2^{2\ell}p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$\gcd(u, v) = 1 \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1 \text{ or } 5.$$

$$x^{2n} + 2^{2\ell}p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$\gcd(u, v) = 1 \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1 \text{ or } 5.$$

$$\text{and } \gcd(v, v^4 - 10u^2v^2 + 5u^4) = 1 \text{ or } 5.$$

$$x^{2n} + 2^{2\ell} p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$\gcd(u, v) = 1 \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1 \text{ or } 5.$$

$$\text{and } \gcd(v, v^4 - 10u^2v^2 + 5u^4) = 1 \text{ or } 5.$$

$u \not\equiv v \pmod 2$

$$x^{2n} + 2^{2\ell} p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$\gcd(u, v) = 1 \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1 \text{ or } 5.$$

$$\text{and } \gcd(v, v^4 - 10u^2v^2 + 5u^4) = 1 \text{ or } 5.$$

$u \not\equiv v \pmod 2 \implies v^4 - 10u^2v^2 + 5u^4$ is odd

$$x^{2n} + 2^{2\ell} p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$\gcd(u, v) = 1 \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1 \text{ or } 5.$$

$$\text{and } \gcd(v, v^4 - 10u^2v^2 + 5u^4) = 1 \text{ or } 5.$$

$$u \not\equiv v \pmod 2 \implies v^4 - 10u^2v^2 + 5u^4 \text{ is odd} \implies 2^\ell | v.$$

$$x^{2n} + 2^{2\ell}p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$\gcd(u, v) = 1 \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1 \text{ or } 5.$$

$$\text{and } \gcd(v, v^4 - 10u^2v^2 + 5u^4) = 1 \text{ or } 5.$$

$$u \not\equiv v \pmod{2} \implies v^4 - 10u^2v^2 + 5u^4 \text{ is odd} \implies 2^\ell | v.$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}$$

for $j \in \mathbb{Z}$,

$$x^{2n} + 2^{2\ell} p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$\gcd(u, v) = 1 \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1 \text{ or } 5.$$

$$\text{and } \gcd(v, v^4 - 10u^2v^2 + 5u^4) = 1 \text{ or } 5.$$

$$u \not\equiv v \pmod 2 \implies v^4 - 10u^2v^2 + 5u^4 \text{ is odd} \implies 2^\ell | v.$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}$$

for $j \in \mathbb{Z}$, where $j = m - 1$ when $p = 5$

$$x^{2n} + 2^{2\ell}p^{2m} = z^5 \implies (x^n)^2 + \left(2^\ell p^m\right)^2 = z^5$$

Apply Lemma, $\exists\, u, v \in \mathbb{Z} - \{0\}$ coprime, opposite parity s.t.

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad \text{and} \quad 2^\ell p^m = v(v^4 - 10u^2v^2 + 5u^4).$$

$$\gcd(u, v) = 1 \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1 \text{ or } 5.$$

$$\text{and } \gcd(v, v^4 - 10u^2v^2 + 5u^4) = 1 \text{ or } 5.$$

$$u \not\equiv v \pmod 2 \implies v^4 - 10u^2v^2 + 5u^4 \text{ is odd} \implies 2^\ell | v.$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}$$

for $j \in \mathbb{Z}$, where $j = m - 1$ when $p = 5$ and $j = 0$ otherwise.

Case I: $n \geq 7$: Modular Approach

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$,

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Completing the square,

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Completing the square, using $20v^4 = 2^{4\ell+2}5^{4j+1}$ with $w \equiv u^2 - 5v^2$,

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Completing the square, using $20v^4 = 2^{4\ell+2}5^{4j+1}$ with $w \equiv u^2 - 5v^2$,

$$B^n + 2^{4\ell+2}5^{4j+1} = w^2$$

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Completing the square, using $20v^4 = 2^{4\ell+2}5^{4j+1}$ with $w \equiv u^2 - 5v^2$,

$$B^n + 2^{4\ell+2}5^{4j+1} = w^2 \implies B^n + 2^{r_1}5^{r_2}(2^{k_1}5^{k_2})^n = w^2$$

for $0 \leq r_1, r_2 < n$.

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Completing the square, using $20v^4 = 2^{4\ell+2}5^{4j+1}$ with $w \equiv u^2 - 5v^2$,

$$B^n + 2^{4\ell+2}5^{4j+1} = w^2 \implies B^n + 2^{r_1}5^{r_2}(2^{k_1}5^{k_2})^n = w^2$$

for $0 \leq r_1, r_2 < n$.

- For primes q, $v_q(2^{r_1}5^{r_2}) \leq \max\{r_1, r_2\} < n$.

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Completing the square, using $20v^4 = 2^{4\ell+2}5^{4j+1}$ with $w \equiv u^2 - 5v^2$,

$$B^n + 2^{4\ell+2}5^{4j+1} = w^2 \implies B^n + 2^{r_1}5^{r_2}(2^{k_1}5^{k_2})^n = w^2$$

for $0 \leq r_1, r_2 < n$.

- For primes q, $v_q(2^{r_1}5^{r_2}) \leq \max\{r_1, r_2\} < n$.
- $v_2(2^{4\ell+2}5^{4j+1}) = 4\ell + 2 \geq 6$.

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Completing the square, using $20v^4 = 2^{4\ell+2}5^{4j+1}$ with $w \equiv u^2 - 5v^2$,

$$B^n + 2^{4\ell+2}5^{4j+1} = w^2 \implies B^n + 2^{r_1}5^{r_2}(2^{k_1}5^{k_2})^n = w^2$$

for $0 \leq r_1, r_2 < n$.

- For primes q, $v_q(2^{r_1}5^{r_2}) \leq \max\{r_1, r_2\} < n$.
- $v_2(2^{4\ell+2}5^{4j+1}) = 4\ell + 2 \geq 6$.
- $2^{4\ell+2}5^{4j+1} \pm 1$ is not a square $\implies 2^{k_1}5^{k_2}B \neq \pm 1$.

Case I: $n \geq 7$: Modular Approach

If $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$ and $\exists A, B \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n,$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}.$$

Completing the square, using $20v^4 = 2^{4\ell+2}5^{4j+1}$ with $w \equiv u^2 - 5v^2$,

$$B^n + 2^{4\ell+2}5^{4j+1} = w^2 \implies B^n + 2^{r_1}5^{r_2}(2^{k_1}5^{k_2})^n = w^2$$

for $0 \leq r_1, r_2 < n$.

- For primes q, $v_q(2^{r_1}5^{r_2}) \leq \max\{r_1, r_2\} < n$.
- $v_2(2^{4\ell+2}5^{4j+1}) = 4\ell + 2 \geq 6$.
- $2^{4\ell+2}5^{4j+1} \pm 1$ is not a square $\implies 2^{k_1}5^{k_2}B \neq \pm 1$.

Apply Bennett-Skinner with $n \geq 7$, prime.

Applying Bennett-Skinner with $n \geq 7$, prime,

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$E: \quad Y^2 + XY = X^3 + \frac{w-1}{4}X^2 + 2^{4\ell-4}5^{4j+1}X,$$

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$E: \quad Y^2 + XY = X^3 + \frac{w-1}{4}X^2 + 2^{4\ell-4}5^{4j+1}X,$$

and $E \sim_n f$ for some newform f of level

$$N = \begin{cases} 1, & \text{if } r_1 = 6 \text{ and } r_2 = 0, \\ 2, & \text{if } r_1 \neq 6 \text{ and } r_2 = 0, \\ 5, & \text{if } r_1 = 6 \text{ and } r_2 \neq 0, \\ 10, & \text{if } r_1 \neq 6 \text{ and } r_2 \neq 0. \end{cases}$$

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$E: \quad Y^2 + XY = X^3 + \frac{w-1}{4}X^2 + 2^{4\ell-4}5^{4j+1}X,$$

and $E \sim_n f$ for some newform f of level

$$N = \begin{cases} 1, & \text{if } r_1 = 6 \text{ and } r_2 = 0, \\ 2, & \text{if } r_1 \neq 6 \text{ and } r_2 = 0, \\ 5, & \text{if } r_1 = 6 \text{ and } r_2 \neq 0, \\ 10, & \text{if } r_1 \neq 6 \text{ and } r_2 \neq 0. \end{cases}$$

However, there are no newforms of level $1, 2, 5$, or 10.

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$E: \quad Y^2 + XY = X^3 + \frac{w-1}{4}X^2 + 2^{4\ell-4}5^{4j+1}X,$$

and $E \sim_n f$ for some newform f of level

$$N = \begin{cases} 1, & \text{if } r_1 = 6 \text{ and } r_2 = 0, \\ 2, & \text{if } r_1 \neq 6 \text{ and } r_2 = 0, \\ 5, & \text{if } r_1 = 6 \text{ and } r_2 \neq 0, \\ 10, & \text{if } r_1 \neq 6 \text{ and } r_2 \neq 0. \end{cases}$$

However, there are no newforms of level $1, 2, 5$, or 10. Hence $5|u$.

Modular Approach Continued

$$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$$

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$.

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$.
Then $j = 0$ and $p \neq 5$.

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$. Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$.
Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$

$$v = \pm 2^\ell p^j \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^{m-j}$$

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$.
Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$
$$v = \pm 2^\ell \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^m$$

Completing the square,

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$.
Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$
$$v = \pm 2^\ell \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^m$$

Completing the square, with $5w_1 = u^2 - 5v^2$,

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$.
Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$

$$v = \pm 2^\ell \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^m$$

Completing the square, with $5w_1 = u^2 - 5v^2$,

$$D^n + 2^{4\ell+2} = 5w_1^2$$

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$. Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$

$$v = \pm 2^\ell \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^m$$

Completing the square, with $5w_1 = u^2 - 5v^2$,

$$D^n + 2^{4\ell+2} = 5w_1^2 \implies D^n + 2^r(2^k)^n = 5w_1^2$$

with $0 \leq r < n$.

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u,v) = 1 \implies 5 \nmid v$. Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$
$$v = \pm 2^\ell \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^m$$

Completing the square, with $5w_1 = u^2 - 5v^2$,

$$D^n + 2^{4\ell+2} = 5w_1^2 \implies D^n + 2^r(2^k)^n = 5w_1^2$$

with $0 \leq r < n$.

- For all primes q, $v_q(2^r) \leq r < n$.

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u,v) = 1 \implies 5 \nmid v$. Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$
$$v = \pm 2^\ell \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^m$$

Completing the square, with $5w_1 = u^2 - 5v^2$,

$$D^n + 2^{4\ell+2} = 5w_1^2 \implies D^n + 2^r(2^k)^n = 5w_1^2$$

with $0 \leq r < n$.

- For all primes q, $v_q(2^r) \leq r < n$.
- Since $\ell \geq 1$, $v_2(2^{4\ell+2}) \geq 6$.

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$.
Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$
$$v = \pm 2^\ell \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^m$$

Completing the square, with $5w_1 = u^2 - 5v^2$,

$$D^n + 2^{4\ell+2} = 5w_1^2 \implies D^n + 2^r(2^k)^n = 5w_1^2$$

with $0 \le r < n$.

- For all primes q, $v_q(2^r) \le r < n$.
- Since $\ell \ge 1$, $v_2(2^{4\ell+2}) \ge 6$.
- $5D^n \equiv 1 \pmod 8$ and so $D \neq \pm 1$.

Modular Approach Continued

$5|u \implies \gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$ and $\gcd(u, v) = 1 \implies 5 \nmid v$.
Then $j = 0$ and $p \neq 5$. Thus $\exists\, C, D \in \mathbb{Z} - \{0\}$ coprime s.t.

$$u = 5^{n-1}C^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5D^n$$
$$v = \pm 2^\ell \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^m$$

Completing the square, with $5w_1 = u^2 - 5v^2$,

$$D^n + 2^{4\ell+2} = 5w_1^2 \implies D^n + 2^r(2^k)^n = 5w_1^2$$

with $0 \leq r < n$.

- For all primes q, $v_q(2^r) \leq r < n$.
- Since $\ell \geq 1$, $v_2(2^{4\ell+2}) \geq 6$.
- $5D^n \equiv 1 \pmod 8$ and so $D \neq \pm 1$.

Again, apply Bennett-Skinner for $n \geq 7$.

Applying Bennett-Skinner with $n \geq 7$, prime,

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2}X^2 + 2^{4\ell-4}5X$$

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2} X^2 + 2^{4\ell-4} 5X$$

with $M' = 2^\alpha 5^2 rad(D)$.

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2} X^2 + 2^{4\ell - 4} 5X$$

with $M' = 2^{\alpha} 5^2 rad(D)$. $F \sim_n g$ for newform g of level

$$M = \begin{cases} 25, & \text{if } r = 6, \\ 50, & \text{if } r \neq 6. \end{cases}$$

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2} X^2 + 2^{4\ell - 4} 5X$$

with $M' = 2^{\alpha} 5^2 rad(D)$. $F \sim_n g$ for newform g of level

$$M = \begin{cases} 25, & \text{if } r = 6, \\ 50, & \text{if } r \neq 6. \end{cases}$$

Thus $M = 50$.

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2} X^2 + 2^{4\ell-4} 5X$$

with $M' = 2^{\alpha} 5^2 rad(D)$. $F \sim_n g$ for newform g of level

$$M = \begin{cases} 25, & \text{if } r = 6, \\ 50, & \text{if } r \neq 6. \end{cases}$$

Thus $M = 50$. Newforms of level 50 are

$$g_1 = q - q^2 + q^3 + q^4 - q^6 + \dots$$

and

$$g_2 = q + q^2 - q^3 + q^4 - q^6 + \dots.$$

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2} X^2 + 2^{4\ell - 4} 5X$$

with $M' = 2^\alpha 5^2 rad(D)$. $F \sim_n g$ for newform g of level

$$M = \begin{cases} 25, & \text{if } r = 6, \\ 50, & \text{if } r \neq 6. \end{cases}$$

Thus $M = 50$. Newforms of level 50 are

$$g_1 = q - q^2 + q^3 + q^4 - q^6 + \dots$$

and

$$g_2 = q + q^2 - q^3 + q^4 - q^6 + \dots.$$

correspond to elliptic curves, F_1 and F_2, defined over $\mathbb{Q}$.

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2}X^2 + 2^{4\ell-4}5X$$

with $M' = 2^{\alpha}5^2 rad(D)$. $F \sim_n g$ for newform g of level

$$M = \begin{cases} 25, & \text{if } r = 6, \\ 50, & \text{if } r \neq 6. \end{cases}$$

Thus $M = 50$. Newforms of level 50 are

$$g_1 = q - q^2 + q^3 + q^4 - q^6 + \dots$$

and

$$g_2 = q + q^2 - q^3 + q^4 - q^6 + \dots.$$

correspond to elliptic curves, F_1 and F_2, defined over $\mathbb{Q}$.

$g = g_i$

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2}X^2 + 2^{4\ell-4}5X$$

with $M' = 2^\alpha 5^2 rad(D)$. $F \sim_n g$ for newform g of level

$$M = \begin{cases} 25, & \text{if } r = 6, \\ 50, & \text{if } r \neq 6. \end{cases}$$

Thus $M = 50$. Newforms of level 50 are

$$g_1 = q - q^2 + q^3 + q^4 - q^6 + \dots$$

and

$$g_2 = q + q^2 - q^3 + q^4 - q^6 + \dots.$$

correspond to elliptic curves, F_1 and F_2, defined over $\mathbb{Q}$.

$g = g_i$ and corresponds to F_i for $i = 1$ or 2.

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2} X^2 + 2^{4\ell - 4} 5X$$

with $M' = 2^{\alpha} 5^2 rad(D)$. $F \sim_n g$ for newform g of level

$$M = \begin{cases} 25, & \text{if } r = 6, \\ 50, & \text{if } r \neq 6. \end{cases}$$

Thus $M = 50$. Newforms of level 50 are

$$g_1 = q - q^2 + q^3 + q^4 - q^6 + \dots$$

and

$$g_2 = q + q^2 - q^3 + q^4 - q^6 + \dots.$$

correspond to elliptic curves, F_1 and F_2, defined over $\mathbb{Q}$.

$g = g_i$ and corresponds to F_i for $i = 1$ or 2.

Since $3 \nmid 50$, $c_3(g) = a_3(F_i)$.

Applying Bennett-Skinner with $n \geq 7$, prime, we have

$$F: \quad Y^2 + XY = X^3 + \frac{5w_1 - 1}{2} X^2 + 2^{4\ell - 4} 5X$$

with $M' = 2^\alpha 5^2 rad(D)$. $F \sim_n g$ for newform g of level

$$M = \begin{cases} 25, & \text{if } r = 6, \\ 50, & \text{if } r \neq 6. \end{cases}$$

Thus $M = 50$. Newforms of level 50 are

$$g_1 = q - q^2 + q^3 + q^4 - q^6 + \dots$$

and

$$g_2 = q + q^2 - q^3 + q^4 - q^6 + \dots.$$

correspond to elliptic curves, F_1 and F_2, defined over $\mathbb{Q}$.

$g = g_i$ and corresponds to F_i for $i = 1$ or 2.

Since $3 \nmid 50$, $c_3(g) = a_3(F_i)$. Thus $a_3(F_i) = \pm 1$.

From Bennett-Skinner, F has nontrivial 2-torsion.

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even.

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3}$$

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$.

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

$3 \nmid rad(D)$

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

$$3 \nmid rad(D) \implies a_3(F) \equiv a_3(F_i) = \pm 1 \pmod{n}.$$

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

$3 \nmid rad(D) \implies a_3(F) \equiv a_3(F_i) = \pm 1 \pmod{n}$. Thus $n \leq 3$.

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

$3 \nmid rad(D) \implies a_3(F) \equiv a_3(F_i) = \pm 1 \pmod{n}$. Thus $n \leq 3$.

$3 | rad(D)$

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

$3 \nmid rad(D) \implies a_3(F) \equiv a_3(F_i) = \pm 1 \pmod{n}$. Thus $n \leq 3$.

$3 | rad(D) \implies \pm 1 \equiv a_3(F_i) \equiv \pm 4 \pmod{n}$.

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \le a_3(F) \le 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

$3 \nmid rad(D) \implies a_3(F) \equiv a_3(F_i) = \pm 1 \pmod{n}$. Thus $n \le 3$.

$3 | rad(D) \implies \pm 1 \equiv a_3(F_i) \equiv \pm 4 \pmod{n}$. Then $n \le 5$.

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \leq a_3(F) \leq 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

$3 \nmid rad(D) \implies a_3(F) \equiv a_3(F_i) = \pm 1 \pmod{n}$. Thus $n \leq 3$.

$3 | rad(D) \implies \pm 1 \equiv a_3(F_i) \equiv \pm 4 \pmod{n}$. Then $n \leq 5$.

Contradictions in both cases.

From Bennett-Skinner, F has nontrivial 2-torsion. Thus

$$F_t(\mathbb{Q}) \text{ contains a point of order } 2 \implies 2 \text{ divides } |\overline{F}(\mathbb{F}_3)|.$$

Hence $a_3(F) = (3+1) - |\overline{F}(\mathbb{F}_3)|$ is even. Further,

$$-2\sqrt{3} \le a_3(F) \le 2\sqrt{3} \implies a_3(F) \in \{-2, 0, 2\}.$$

Recall that $F \sim_n g$, thus $F \sim_n F_i$. By Lemma,

$$a_3(F_i) \equiv \begin{cases} a_3(F) \pmod{n}, & \text{if } 3 \nmid rad(D), \\ \pm 4 \pmod{n}, & \text{if } 3 | rad(D). \end{cases}$$

$3 \nmid rad(D) \implies a_3(F) \equiv a_3(F_i) = \pm 1 \pmod{n}$. Thus $n \le 3$.

$3|rad(D) \implies \pm 1 \equiv a_3(F_i) \equiv \pm 4 \pmod{n}$. Then $n \le 5$.

Contradictions in both cases. Hence $n \in \{2, 3, 5\}$.

Theorem (G-)

The equation

$$X^{2N} + 2^{2L}p^{2M} = Z^5$$

has no solution for odd prime p, *with* X, Z, N, L, $M \in \mathbb{Z}^+$, $N > 1$, *and* $\gcd(X, Z, 2p) = 1$.