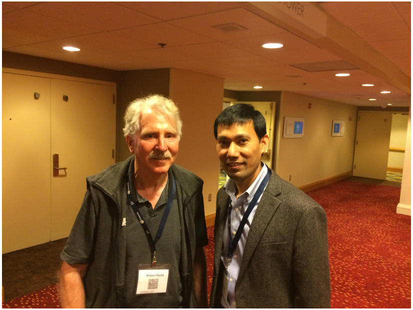
Recent Developments on Gassmann Equivalence in Groups

Bir Kafle
(Joint work with R. Litherland, R. Perlis and M. Somadi)

Math/Stat/CS Department
Purdue University Northwest

Southern Regional Number Theory Conference
Baton Rouge, LA, April 08-09, 2017


EXIT
Department of
Mathematics



Timeline - Hurwitz

- 1859 Born.
- 1881 Doctorate under Felix Klein.
- 1892 Frobenius's successor, ETH Zurich.
- 1919 Died, leaving many unpublished notebooks.
- George Polya drew attention to the contents.

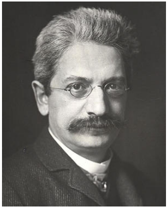


Figure: Adolf Hurwitz

Pic. Source - *library.ethz.ch/en/Resources*

Timeline - Gassmann

- Fritz Gassmann (1899 – 1990).
- Swiss mathematician and geophysicist.
- In 1926, Gassmann published one set of Hurwitz's notes followed by Gassmann's interpretation of what Hurwitz meant.

Gassmann's Condition

- Throughout, H and H' will denote subgroups of a finite group G.
- In Gassmann's paper, the following group-theoretic condition appeared:

$$|c \cap H| = |c \cap H'| \tag{1}$$

for any conjugacy class c in G.
- When (1) holds, H and H' are called *Gassmann equivalent* in G.
- We call (G, H, H'), a *Gassmann triple*.
- If H, H' are conjugate in G, then (G, H, H') is *trivial* Gassmann triple. e.g. Cyclic Gassmann equivalent subgroups.

Gassmann's Condition

- Throughout, H and H' will denote subgroups of a finite group G.
- In Gassmann's paper, the following group-theoretic condition appeared:

$$|c \cap H| = |c \cap H'| \tag{1}$$

for any conjugacy class c in G.

- When (1) holds, H and H' are called *Gassmann equivalent* in G.
- We call (G, H, H'), a *Gassmann triple*.
- If H, H' are conjugate in G, then (G, H, H') is *trivial* Gassmann triple. e.g. Cyclic Gassmann equivalent subgroups.

Gassmann's Condition

- Throughout, H and H' will denote subgroups of a finite group G.
- In Gassmann's paper, the following group-theoretic condition appeared:

$$|c \cap H| = |c \cap H'| \tag{1}$$

  for any conjugacy class c in G.
- When (1) holds, H and H' are called *Gassmann equivalent* in G.
- We call (G, H, H'), a *Gassmann triple*.
- If H, H' are conjugate in G, then (G, H, H') is *trivial* Gassmann triple. e.g. Cyclic Gassmann equivalent subgroups.

Some Results

Theorem (Lenstra, 2000)

For every positive integer n, the following are equivalent.

1. *There exists a finite solvable group G with two nontrivial Gassmann equivalent subgroups of index n.*
2. *There are prime numbers p, q, r with $pqr|n$ and $p|q(q-1)$.*

Some Results

Theorem (Feit, 1980)

Let (G, H, H') *be a nontrivial Gassmann triple of prime index* p. *Then either*
$p = 11$ *or,*
$$p = \frac{q^k - 1}{q - 1},$$
for some prime power q *and some* $k \geq 3$.

Some Results

Theorem (de Smit, 2003)

For every odd prime p, there is a nontrivial Gassmann triple of index $n = 2p + 2$.

Some Results

Theorem (Perlis, 1977)

If H and H' are Gassmann equivalent in G and $(G : H) \leq 6$, then H is conjugate in G to H'.

Some Results

- Two finite groups are said to have the same order type if they have the same number of elements of any given order.

Example

Two subgroups $H = \langle (12)(345) \rangle$, and $H' = \langle (12345) \rangle$ of $G = S_6$ have the same ordere type.

- Gassmann equivalent subgroups have the same order type.

Theorem

Two finite abelian groups G and G' with the same order type are isomorphic.

Some Results

- Two finite groups are said to have the same order type if they have the same number of elements of any given order.

Example

Two subgroups $H = \langle(12)(345)\rangle$, and $H' = \langle(12345)\rangle$ of $G = S_6$ have the same ordere type.

- Gassmann equivalent subgroups have the same order type.

Theorem

Two finite abelian groups G and G' with the same order type are isomorphic.

Some Results

Theorem

For every natural number n, there exists a finite group G with $n+1$ pairwise non-conjugate subgroups $H_0, H_1, \cdots, H_n$ such that H_i and H_j are Gassmann equivalent in G for all $i, j = 0, 1, \cdots, n$.

Some Results

Let (G, H, H') be a Gassmann triple and M be a normal subgroup of G. Then

- $H \cap M$ and $H' \cap M$ are Gassmann equivalent in G.
- HM and $H'M$ are Gassmann equivalent in G.

Some Results

Let (G, H, H') be a Gassmann triple and M be a normal subgroup of G. Then

- $H \cap M$ and $H' \cap M$ are Gassmann equivalent in G.
- HM and $H'M$ are Gassmann equivalent in G.

Bijective Local Conjugacy

Definition

Two subgroups H and H' of G are called *bijectively locally conjugate* in G if there exists a bijection $\varphi : H \longrightarrow H'$ such that h and $\varphi(h)$ are conjugate in G for any $h \in H$.

Example

- Consider the group

$$G = (\mathbb{Z}/8\mathbb{Z})^* \ltimes \mathbb{Z}/8\mathbb{Z} = \{(h,k) | \, h = 1,3,5,7; k = 0,1,2,\ldots,7\}$$

with the operation defined by

$$(x,y)(h,k) = (xh, hy + k).$$

Let

$$H = \{(1,0),(3,0),(5,0),(7,0)\}$$

$$H' = \{(1,0),(3,4),(5,4),(7,0)\}.$$

- Mapping vertically gives a multiplicative bijective local conjugation $\varphi : H \longrightarrow H'$ in G, which is not a global conjugation.

Example

- Consider the group

$$G = (\mathbb{Z}/8\mathbb{Z})^* \ltimes \mathbb{Z}/8\mathbb{Z} = \{(h,k)|\, h = 1,3,5,7; k = 0,1,2,\ldots,7\}$$

with the operation defined by

$$(x,y)(h,k) = (xh, hy+k).$$

Let

$$H = \{(1,0),(3,0),(5,0),(7,0)\}$$
$$H' = \{(1,0),(3,4),(5,4),(7,0)\}.$$

- Mapping vertically gives a multiplicative bijective local conjugation $\varphi : H \longrightarrow H'$ in G, which is not a global conjugation.

Example

- Consider the group

$$G = (\mathbb{Z}/8\mathbb{Z})^* \ltimes \mathbb{Z}/8\mathbb{Z} = \{(h,k) | \, h = 1,3,5,7; k = 0,1,2,\ldots,7\}$$

with the operation defined by

$$(x,y)(h,k) = (xh, hy+k).$$

Let

$$H = \{(1,0),(3,0),(5,0),(7,0)\}$$

$$H' = \{(1,0),(3,4),(5,4),(7,0)\}.$$

- Mapping vertically gives a multiplicative bijective local conjugation $\varphi : H \longrightarrow H'$ in G, which is not a global conjugation.

Theorem

The following statements are equivalent:

1. $|g^G \cap H| = |g^G \cap H'|$ *for all* $g \in G$ *(Gassmann's condition).*
2. H *and* H' *are bijectively locally conjugate in* G [*S. Chen*, 1992].
3. *There exists a bijective local conjugation* $\bar{\varphi} : G \longrightarrow G$ *such that* $\bar{\varphi}(H) = H'$.

Theorem

The following statements are equivalent:

1. $|g^G \cap H| = |g^G \cap H'|$ *for all* $g \in G$ *(Gassmann's condition).*
2. H *and* H' *are bijectively locally conjugate in* G [S. Chen, 1992].
3. *There exists a bijective local conjugation* $\bar{\varphi} : G \longrightarrow G$ *such that* $\bar{\varphi}(H) = H'$.

Theorem

The following statements are equivalent:

1. $|g^G \cap H| = |g^G \cap H'|$ *for all* $g \in G$ *(Gassmann's condition).*
2. *H and* H' *are bijectively locally conjugate in G* [S. Chen, 1992].
3. *There exists a bijective local conjugation* $\bar{\varphi} : G \longrightarrow G$ *such that* $\bar{\varphi}(H) = H'$.

Theorem

The following statements are equivalent:

1. $|g^G \cap H| = |g^G \cap H'|$ *for all* $g \in G$ *(Gassmann's condition).*
2. H *and* H' *are bijectively locally conjugate in* G [S. Chen, 1992].
3. *There exists a bijective local conjugation* $\bar{\varphi} : G \longrightarrow G$ *such that* $\bar{\varphi}(H) = H'$.

A Different Approach to Gassmann Equivalence

- Let H be a subgroup of a finite group G.
- For $g \in G$, let π_g be the permutation of G/H given by left multiplication by g.
- Let $\gamma_i = \gamma_i(\pi_g)$ be the number of cycles of π_g of length i.
- Set $\Gamma(\pi_g) = \sum \gamma_i$.
- Let H' be another subgroup of G, and π'_g be the permutation of G/H' given by left multiplication by g.

A Different Approach to Gassmann Equivalence

- Let H be a subgroup of a finite group G.
- For $g \in G$, let π_g be the permutation of G/H given by left multiplication by g.
- Let $\gamma_i = \gamma_i(\pi_g)$ be the number of cycles of π_g of length i.
- Set $\Gamma(\pi_g) = \sum \gamma_i$.
- Let H' be another subgroup of G, and π'_g be the permutation of G/H' given by left multiplication by g.

A Different Approach to Gassmann Equivalence

- Let H be a subgroup of a finite group G.
- For $g \in G$, let π_g be the permutation of G/H given by left multiplication by g.
- Let $\gamma_i = \gamma_i(\pi_g)$ be the number of cycles of π_g of length i.
- Set $\Gamma(\pi_g) = \sum \gamma_i$.
- Let H' be another subgroup of G, and π'_g be the permutation of G/H' given by left multiplication by g.

A Different Approach to Gassmann Equivalence

- Let H be a subgroup of a finite group G.
- For $g \in G$, let π_g be the permutation of G/H given by left multiplication by g.
- Let $\gamma_i = \gamma_i(\pi_g)$ be the number of cycles of π_g of length i.
- Set $\Gamma(\pi_g) = \sum \gamma_i$.
- Let H' be another subgroup of G, and π'_g be the permutation of G/H' given by left multiplication by g.

A Different Approach to Gassmann Equivalence

- Let H be a subgroup of a finite group G.
- For $g \in G$, let π_g be the permutation of G/H given by left multiplication by g.
- Let $\gamma_i = \gamma_i(\pi_g)$ be the number of cycles of π_g of length i.
- Set $\Gamma(\pi_g) = \sum \gamma_i$.
- Let H' be another subgroup of G, and π'_g be the permutation of G/H' given by left multiplication by g.

A Different Approach to Gassmann Equivalence

- Let H be a subgroup of a finite group G.
- For $g \in G$, let π_g be the permutation of G/H given by left multiplication by g.
- Let $\gamma_i = \gamma_i(\pi_g)$ be the number of cycles of π_g of length i.
- Set $\Gamma(\pi_g) = \sum \gamma_i$.
- Let H' be another subgroup of G, and π'_g be the permutation of G/H' given by left multiplication by g.

A Different Approach to Gassmann Equivalence

Theorem

The following statements are equivalent:

1. *H and H' are Gassmann equivalent in G.*
2. *$\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ for all $g \in G$.*
3. *$\gamma_i(\pi_g) = \gamma_i(\pi'_g)$ for all $g \in G$ and for all $i = 1, 2, \cdots, n$.*
4. *$\Gamma(\pi_g) = \Gamma(\pi'_g)$ for all $g \in G$.*

A Different Approach to Gassmann Equivalence

Theorem

The following statements are equivalent:

1. *H and H' are Gassmann equivalent in G.*
2. *$\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ for all $g \in G$.*
3. *$\gamma_i(\pi_g) = \gamma_i(\pi'_g)$ for all $g \in G$ and for all $i = 1, 2, \cdots, n$.*
4. *$\Gamma(\pi_g) = \Gamma(\pi'_g)$ for all $g \in G$.*

A Different Approach to Gassmann Equivalence

Theorem

The following statements are equivalent:

1. H *and* H' *are Gassmann equivalent in* G.
2. $\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ *for all* $g \in G$.
3. $\gamma_i(\pi_g) = \gamma_i(\pi'_g)$ *for all* $g \in G$ *and for all* $i = 1, 2, \cdots, n$.
4. $\Gamma(\pi_g) = \Gamma(\pi'_g)$ *for all* $g \in G$.

A Different Approach to Gassmann Equivalence

Theorem

The following statements are equivalent:

1. *H and H' are Gassmann equivalent in G.*
2. $\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ *for all* $g \in G$.
3. $\gamma_i(\pi_g) = \gamma_i(\pi'_g)$ *for all* $g \in G$ *and for all* $i = 1, 2, \cdots, n$.
4. $\Gamma(\pi_g) = \Gamma(\pi'_g)$ *for all* $g \in G$.

A Different Approach to Gassmann Equivalence

Theorem

The following statements are equivalent:

1. H *and* H' *are Gassmann equivalent in* G.
2. $\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ *for all* $g \in G$.
3. $\gamma_i(\pi_g) = \gamma_i(\pi'_g)$ *for all* $g \in G$ *and for all* $i = 1, 2, \cdots, n$.
4. $\Gamma(\pi_g) = \Gamma(\pi'_g)$ *for all* $g \in G$.

A Different Approach to Gassmann Equivalence

The proof uses the following lemma.

Lemma

For any $\sigma, \tau \in S_n$, the following are equivalent:

1. σ *and* τ *are conjugate in* S_n.
2. $\gamma_1(\sigma^k) = \gamma_1(\tau^k)$ *for all* $k = 1, 2, \cdots, n$.
3. $\gamma_i(\sigma) = \gamma_i(\tau)$ *for all* $i = 1, 2, \cdots, n$.
4. $\Gamma(\sigma^k) = \Gamma(\tau^k)$ *for all* $k = 1, 2, \cdots, n$.

A Different Approach to Gassmann Equivalence

The proof uses the following lemma.

Lemma

For any $\sigma, \tau \in S_n$, the following are equivalent:

1. σ *and* τ *are conjugate in* S_n.
2. $\gamma_1(\sigma^k) = \gamma_1(\tau^k)$ *for all* $k = 1, 2, \cdots, n$.
3. $\gamma_i(\sigma) = \gamma_i(\tau)$ *for all* $i = 1, 2, \cdots, n$.
4. $\Gamma(\sigma^k) = \Gamma(\tau^k)$ *for all* $k = 1, 2, \cdots, n$.

A Different Approach to Gassmann Equivalence

The proof uses the following lemma.

Lemma

For any $\sigma, \tau \in S_n$, the following are equivalent:

1. *σ and τ are conjugate in S_n.*
2. *$\gamma_1(\sigma^k) = \gamma_1(\tau^k)$ for all $k = 1, 2, \cdots, n$.*
3. *$\gamma_i(\sigma) = \gamma_i(\tau)$ for all $i = 1, 2, \cdots, n$.*
4. *$\Gamma(\sigma^k) = \Gamma(\tau^k)$ for all $k = 1, 2, \cdots, n$.*

A Different Approach to Gassmann Equivalence

The proof uses the following lemma.

Lemma

For any $\sigma, \tau \in S_n$, the following are equivalent:

1. σ *and* τ *are conjugate in* S_n.
2. $\gamma_1(\sigma^k) = \gamma_1(\tau^k)$ *for all* $k = 1, 2, \cdots, n$.
3. $\gamma_i(\sigma) = \gamma_i(\tau)$ *for all* $i = 1, 2, \cdots, n$.
4. $\Gamma(\sigma^k) = \Gamma(\tau^k)$ *for all* $k = 1, 2, \cdots, n$.

A Different Approach to Gassmann Equivalence

The proof uses the following lemma.

Lemma

For any $\sigma, \tau \in S_n$, the following are equivalent:

1. σ *and* τ *are conjugate in* S_n.
2. $\gamma_1(\sigma^k) = \gamma_1(\tau^k)$ *for all* $k = 1, 2, \cdots, n$.
3. $\gamma_i(\sigma) = \gamma_i(\tau)$ *for all* $i = 1, 2, \cdots, n$.
4. $\Gamma(\sigma^k) = \Gamma(\tau^k)$ *for all* $k = 1, 2, \cdots, n$.

A Different Approach to Gassmann Equivalence

The proof uses the following lemma.

Lemma

For any $\sigma, \tau \in S_n$, the following are equivalent:

1. *σ and τ are conjugate in S_n.*
2. *$\gamma_1(\sigma^k) = \gamma_1(\tau^k)$ for all $k = 1, 2, \cdots, n$.*
3. *$\gamma_i(\sigma) = \gamma_i(\tau)$ for all $i = 1, 2, \cdots, n$.*
4. *$\Gamma(\sigma^k) = \Gamma(\tau^k)$ for all $k = 1, 2, \cdots, n$.*

A Different Approach to Gassmann Equivalence

Proof.

$(4) \Rightarrow (3)$.

- $\Gamma(\sigma^k) = \sum_{j=1}^{n} \gcd(k,j) \cdot \gamma_j(\sigma)$ for $k = 1, 2, \cdots, n$.
- Set $M = (m_{ij})$, where $m_{ij} = \gcd(i,j)$.
- $(\Gamma(\sigma), \Gamma(\sigma^2), \ldots, \Gamma(\sigma^n)) = (\gamma_1(\sigma), \gamma_2(\sigma), \ldots, \gamma_n(\sigma)) \cdot M$.
- By Smith, 1876, $\det(M) = \varphi(1) \cdot \varphi(2) \cdots \varphi(n) \neq 0$.

A Different Approach to Gassmann Equivalence

Proof.

(4) $\Rightarrow$ (3).

- $\Gamma(\sigma^k) = \sum_{j=1}^{n} \gcd(k,j) \cdot \gamma_j(\sigma)$ for $k = 1, 2, \cdots, n$.
- Set $M = (m_{ij})$, where $m_{ij} = \gcd(i,j)$.
- $(\Gamma(\sigma), \Gamma(\sigma^2), \ldots, \Gamma(\sigma^n)) = (\gamma_1(\sigma), \gamma_2(\sigma), \ldots, \gamma_n(\sigma)) \cdot M$.
- By Smith, 1876, $\det(M) = \varphi(1) \cdot \varphi(2) \cdots \varphi(n) \neq 0$.

A Different Approach to Gassmann Equivalence

Proof.

(4) $\Rightarrow$ (3).

- $\Gamma(\sigma^k) = \sum_{j=1}^{n} \gcd(k,j) \cdot \gamma_j(\sigma)$ for $k = 1, 2, \cdots, n$.
- Set $M = (m_{ij})$, where $m_{ij} = \gcd(i,j)$.
- $(\Gamma(\sigma), \Gamma(\sigma^2), \ldots, \Gamma(\sigma^n)) = (\gamma_1(\sigma), \gamma_2(\sigma), \ldots, \gamma_n(\sigma)) \cdot M$.
- By Smith, 1876, $\det(M) = \varphi(1) \cdot \varphi(2) \cdots \varphi(n) \neq 0$.

A Different Approach to Gassmann Equivalence

Proof.

$(4) \Rightarrow (3)$.

- $\Gamma(\sigma^k) = \sum_{j=1}^{n} \gcd(k, j) \cdot \gamma_j(\sigma)$ for $k = 1, 2, \cdots, n$.
- Set $M = (m_{ij})$, where $m_{ij} = \gcd(i, j)$.
- $(\Gamma(\sigma), \Gamma(\sigma^2), \ldots, \Gamma(\sigma^n)) = (\gamma_1(\sigma), \gamma_2(\sigma), \ldots, \gamma_n(\sigma)) \cdot M$.
- By Smith, 1876, $\det(M) = \varphi(1) \cdot \varphi(2) \cdots \varphi(n) \neq 0$.

A Different Approach to Gassmann Equivalence

Proof.

(4) $\Rightarrow$ (3).

- $\Gamma(\sigma^k) = \sum_{j=1}^{n} \gcd(k,j) \cdot \gamma_j(\sigma)$ for $k = 1, 2, \cdots, n$.
- Set $M = (m_{ij})$, where $m_{ij} = \gcd(i,j)$.
- $(\Gamma(\sigma), \Gamma(\sigma^2), \ldots, \Gamma(\sigma^n)) = (\gamma_1(\sigma), \gamma_2(\sigma), \ldots, \gamma_n(\sigma)) \cdot M$.
- By Smith, 1876, $\det(M) = \varphi(1) \cdot \varphi(2) \cdots \varphi(n) \neq 0$.

A Different Approach to Gassmann Equivalence

Proof.

(4) $\Rightarrow$ (3).

- $\Gamma(\sigma^k) = \sum_{j=1}^{n} \gcd(k,j) \cdot \gamma_j(\sigma)$ for $k = 1, 2, \cdots, n$.
- Set $M = (m_{ij})$, where $m_{ij} = \gcd(i,j)$.
- $(\Gamma(\sigma), \Gamma(\sigma^2), \ldots, \Gamma(\sigma^n)) = (\gamma_1(\sigma), \gamma_2(\sigma), \ldots, \gamma_n(\sigma)) \cdot M$.
- By Smith, 1876, $\det(M) = \varphi(1) \cdot \varphi(2) \cdots \varphi(n) \neq 0$.

Reformulations of Gassmann Equivalence

Lemma

Let H, H' be subgroups of a finite group G. The following statements are equivalent:

1. H, H' *satisfy Gassmann's condition in* G.
2. H, H' *are bijectively locally conjugate in* G.
3. *There exists a bijective local conjugation* $\bar{\varphi} : G \longrightarrow G$ *such that* $\bar{\varphi}(H) = H'$.
4. $\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ *as* $\mathbb{Q}[G]$*-modules.*
5. $\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ *for all* $g \in G$.

Reformulations of Gassmann Equivalence

Lemma

Let H, H' be subgroups of a finite group G. The following statements are equivalent:

1. H, H' *satisfy Gassmann's condition in* G.
2. H, H' *are bijectively locally conjugate in* G.
3. *There exists a bijective local conjugation* $\bar{\varphi} : G \longrightarrow G$ *such that* $\bar{\varphi}(H) = H'$.
4. $\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ *as* $\mathbb{Q}[G]$*-modules.*
5. $\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ *for all* $g \in G$.

Reformulations of Gassmann Equivalence

Lemma

Let H, H' be subgroups of a finite group G. The following statements are equivalent:

1. H, H' *satisfy Gassmann's condition in* G.
2. H, H' *are bijectively locally conjugate in* G.
3. *There exists a bijective local conjugation* $\bar{\varphi} : G \longrightarrow G$ *such that* $\bar{\varphi}(H) = H'$.
4. $\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ *as* $\mathbb{Q}[G]$*-modules.*
5. $\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ *for all* $g \in G$.

Reformulations of Gassmann Equivalence

Lemma

Let H, H' be subgroups of a finite group G. The following statements are equivalent:

1. *H, H' satisfy Gassmann's condition in G.*
2. *H, H' are bijectively locally conjugate in G.*
3. *There exists a bijective local conjugation $\bar{\varphi} : G \longrightarrow G$ such that $\bar{\varphi}(H) = H'$.*
4. *$\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ as $\mathbb{Q}[G]$-modules.*
5. *$\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ for all $g \in G$.*

Reformulations of Gassmann Equivalence

Lemma

Let H, H' be subgroups of a finite group G. The following statements are equivalent:

1. *H, H' satisfy Gassmann's condition in G.*
2. *H, H' are bijectively locally conjugate in G.*
3. *There exists a bijective local conjugation $\bar{\varphi} : G \longrightarrow G$ such that $\bar{\varphi}(H) = H'$.*
4. *$\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ as $\mathbb{Q}[G]$-modules.*
5. *$\gamma_1(\pi_g) = \gamma_1(\pi'_g)$ for all $g \in G$.*

Reformulations of Gassmann Equivalence

Lemma (cont.)

6. *coset type* $[G \bmod (H, C)]$ = *coset type* $[G \bmod (H', C)]$ *for any cyclic subgroup* C *of* G.
7. $\Gamma(\pi_g) = \Gamma(\pi'_g)$ *for all* $g \in G$.
8. π_g *and* π'_g *have the same cycle length sequence for all* $g \in G$ *(sequence of lengths of cycles in factorization of* π_g *and* π'_g*).*
9. π_g *and* π'_g *have the same cycle number sequence for all* $g \in G$.
10. $(G : H) = (G : H') = n$ *and* π_g, π'_g *are conjugate in* S_n*, for all* $g \in G$.

Reformulations of Gassmann Equivalence

Lemma (cont.)

6. *coset type* $[G \bmod (H, C)]$ = *coset type* $[G \bmod (H', C)]$ *for any cyclic subgroup* C *of* G.
7. $\Gamma(\pi_g) = \Gamma(\pi'_g)$ *for all* $g \in G$.
8. π_g *and* π'_g *have the same cycle length sequence for all* $g \in G$ *(sequence of lengths of cycles in factorization of* π_g *and* π'_g*).*
9. π_g *and* π'_g *have the same cycle number sequence for all* $g \in G$.
10. $(G : H) = (G : H') = n$ *and* π_g, π'_g *are conjugate in* S_n, *for all* $g \in G$.

Reformulations of Gassmann Equivalence

Lemma (cont.)

6. *coset type* $[G \bmod (H, C)]$ = *coset type* $[G \bmod (H', C)]$ *for any cyclic subgroup* C *of* G.
7. $\Gamma(\pi_g) = \Gamma(\pi'_g)$ *for all* $g \in G$.
8. π_g *and* π'_g *have the same cycle length sequence for all* $g \in G$ *(sequence of lengths of cycles in factorization of* π_g *and* π'_g*).*
9. π_g *and* π'_g *have the same cycle number sequence for all* $g \in G$.
10. $(G : H) = (G : H') = n$ *and* π_g, π'_g *are conjugate in* S_n, *for all* $g \in G$.

Reformulations of Gassmann Equivalence

Lemma (cont.)

6. *coset type* $[G \bmod (H, C)]$ = *coset type* $[G \bmod (H', C)]$ *for any cyclic subgroup* C *of* G.
7. $\Gamma(\pi_g) = \Gamma(\pi'_g)$ *for all* $g \in G$.
8. π_g *and* π'_g *have the same cycle length sequence for all* $g \in G$ *(sequence of lengths of cycles in factorization of* π_g *and* π'_g*).*
9. π_g *and* π'_g *have the same cycle number sequence for all* $g \in G$.
10. $(G : H) = (G : H') = n$ *and* π_g, π'_g *are conjugate in* S_n, *for all* $g \in G$.

Reformulations of Gassmann Equivalence

Lemma (cont.)

6. *coset type* $[G \bmod (H, C)]$ = *coset type* $[G \bmod (H', C)]$ *for any cyclic subgroup* C *of* G.
7. $\Gamma(\pi_g) = \Gamma(\pi'_g)$ *for all* $g \in G$.
8. π_g *and* π'_g *have the same cycle length sequence for all* $g \in G$ *(sequence of lengths of cycles in factorization of* π_g *and* π'_g*).*
9. π_g *and* π'_g *have the same cycle number sequence for all* $g \in G$.
10. $(G : H) = (G : H') = n$ *and* π_g, π'_g *are conjugate in* S_n, *for all* $g \in G$.

Applications of Gassmann Equivalence

Gassmann triple (G, H, H') can be used to produce:

- pairs of number fields having identical Dedekind zeta functions.
- pairs of isospectral Riemannian manifolds.
- pairs of nonisomorphic finite graphs with identical Ihara zeta functions.

Arithmetically Equivalent Number Fields

$$
\begin{array}{ccc}
K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t} & \mathcal{O}_K/\mathfrak{p}_i \\
\Big| & \Big| & \Big|\, f_i \\
\mathbb{Q} & p & \mathbb{Z}/p
\end{array}
$$

- Order the primes $\mathfrak{p}_i$ so that $f_i \leq f_{i+1}$.
- $(f_1, f_2, \cdots, f_t)$ = splitting type in K of the prime p.

Arithmetically Equivalent Number Fields

$$
\begin{array}{ccc}
K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t} & \mathcal{O}_K/\mathfrak{p}_i \\
\Big| & \Big| & \Big|\, f_i \\
\mathbb{Q} & p & \mathbb{Z}/p
\end{array}
$$

- Order the primes $\mathfrak{p}_i$ so that $f_i \leq f_{i+1}$.
- $(f_1, f_2, \cdots, f_t)$ = splitting type in K of the prime p.

Arithmetically Equivalent Number Fields

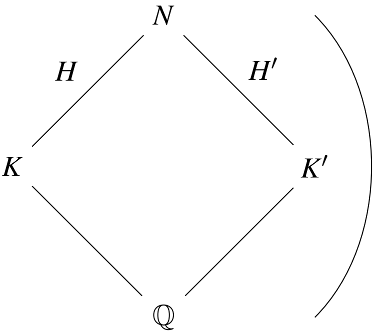
$$
\begin{array}{ccc}
K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t} & \mathcal{O}_K/\mathfrak{p}_i \\
\Big| & \Big| & \Big|\, f_i \\
\mathbb{Q} & p & \mathbb{Z}/p
\end{array}
$$

- Order the primes $\mathfrak{p}_i$ so that $f_i \leq f_{i+1}$.
- $(f_1, f_2, \cdots, f_t)$ = splitting type in K of the prime p.

Arithmetically Equivalent Number Fields

Definition

Two number fields K, K' are said to be arithmetically equivalent if each prime $p \in \mathbb{Z}$ has the same splitting type in K as in K'.



$$G = Gal(N/\mathbb{Q})$$

Perlis' Theorem

Theorem

The following statements are equivalent:

1. $\zeta_K(s) = \zeta_{K'}(s)$.
2. *K, K' are arithmetically equivalent.*
3. *H and H' are Gassmann equivalent in G.*

Perlis' Theorem

Theorem

The following statements are equivalent:

1. $\zeta_K(s) = \zeta_{K'}(s)$.
2. *K, K' are arithmetically equivalent.*
3. *H and H' are Gassmann equivalent in G.*

Perlis' Theorem

Theorem

The following statements are equivalent:

1. $\zeta_K(s) = \zeta_{K'}(s)$.
2. K, K' *are arithmetically equivalent.*
3. H *and* H' *are Gassmann equivalent in* G*.*

Perlis' Theorem

Theorem

The following statements are equivalent:

1. $\zeta_K(s) = \zeta_{K'}(s)$.
2. K, K' *are arithmetically equivalent.*
3. H *and* H' *are Gassmann equivalent in* G.

A New Proof Stuart-Perlis Theorem

Theorem (Stuart and Perlis, 1995)

The following statements are equivalent:

1. *K, K' are arithmetically equivalent.*
2. *Almost every prime number p has the same number of prime ideal factors in K as in K'.*

A New Proof Stuart-Perlis Theorem

Theorem (Stuart and Perlis, 1995)

The following statements are equivalent:

1. K, K' *are arithmetically equivalent.*
2. *Almost every prime number* p *has the same number of prime ideal factors in* K *as in* K'.

A New Proof Stuart-Perlis Theorem

Theorem (Stuart and Perlis, 1995)

The following statements are equivalent:

1. K, K' *are arithmetically equivalent.*
2. *Almost every prime number* p *has the same number of prime ideal factors in* K *as in* K'.

A New Proof Stuart-Perlis Theorem

Proof.

(2) $\Rightarrow$ (1).

- $G = Gal(N/\mathbb{Q})$, $H = Gal(N/K)$ and $H' = Gal(N/K')$.
- For each prime $p \in \mathbb{Z}$ unramified in N, choose a prime $\mathfrak{Q}$ of N lying over p.
- Let $\sigma_{\mathfrak{Q}}$ be the Frobenius automorphism of $\mathfrak{Q}/p$, defined by

$$\sigma_{\mathfrak{Q}}(a) \equiv a^p \bmod \mathfrak{Q}$$

for all $a \in \mathcal{O}_N$.

A New Proof Stuart-Perlis Theorem

Proof.

(2) $\Rightarrow$ (1).

- $G = Gal(N/\mathbb{Q})$, $H = Gal(N/K)$ and $H' = Gal(N/K')$.
- For each prime $p \in \mathbb{Z}$ unramified in N, choose a prime $\mathfrak{Q}$ of N lying over p.
- Let $\sigma_{\mathfrak{Q}}$ be the Frobenius automorphism of $\mathfrak{Q}/p$, defined by

$$\sigma_{\mathfrak{Q}}(a) \equiv a^p \bmod \mathfrak{Q}$$

for all $a \in \mathcal{O}_N$.

A New Proof Stuart-Perlis Theorem

Proof.

(2) $\Rightarrow$ (1).

- $G = Gal(N/\mathbb{Q})$, $H = Gal(N/K)$ and $H' = Gal(N/K')$.
- For each prime $p \in \mathbb{Z}$ unramified in N, choose a prime $\mathfrak{Q}$ of N lying over p.
- Let $\sigma_{\mathfrak{Q}}$ be the Frobenius automorphism of $\mathfrak{Q}/p$, defined by

$$\sigma_{\mathfrak{Q}}(a) \equiv a^p \bmod \mathfrak{Q}$$

for all $a \in \mathcal{O}_N$.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- Let $K = \mathbb{Q}(\alpha)/\mathbb{Q}$ be a finite extension of number fields, $N/\mathbb{Q}$ a Galois extension with $K \subset N$ and $G = Gal(N/\mathbb{Q})$. For any prime number p which is unramified in N the following statements are equivalent:

  1. p has splitting type $(f_1, f_2, \ldots, f_t)$ in K.
  2. For any prime $\mathfrak{Q}$ of N lying over p, the Frobenius automorphism $\sigma_{\mathfrak{Q}}$ acting on the n conjugates of α has cycle length sequence $(f_1, f_2, \ldots, f_t)$.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- Let $K = \mathbb{Q}(\alpha)/\mathbb{Q}$ be a finite extension of number fields, $N/\mathbb{Q}$ a Galois extension with $K \subset N$ and $G = Gal(N/\mathbb{Q})$. For any prime number p which is unramified in N the following statements are equivalent:
  1. p has splitting type $(f_1, f_2, \ldots, f_t)$ in K.
  2. For any prime $\mathfrak{Q}$ of N lying over p, the Frobenius automorphism $\sigma_{\mathfrak{Q}}$ acting on the n conjugates of α has cycle length sequence $(f_1, f_2, \ldots, f_t)$.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- Let $K = \mathbb{Q}(\alpha)/\mathbb{Q}$ be a finite extension of number fields, $N/\mathbb{Q}$ a Galois extension with $K \subset N$ and $G = Gal(N/\mathbb{Q})$. For any prime number p which is unramified in N the following statements are equivalent:
  1. p has splitting type $(f_1, f_2, \ldots, f_t)$ in K.
  2. For any prime $\mathfrak{Q}$ of N lying over p, the Frobenius automorphism $\sigma_{\mathfrak{Q}}$ acting on the n conjugates of α has cycle length sequence $(f_1, f_2, \ldots, f_t)$.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- It is given that $\Gamma(\pi_{\sigma_{\mathfrak{Q}}}) = \Gamma(\pi'_{\sigma_{\mathfrak{Q}}})$.
- Take $\omega \in G$.
- By Chebotarev Density Theorem, there exists a prime p unramified in N, and a prime $\mathfrak{Q}$ of N lying over p with $\sigma_{\mathfrak{Q}} = \omega$.
- So $\Gamma(\pi_{\omega}) = \Gamma(\pi'_{\omega})$.
- ω is an arbitrary.
- H and H' are Gassmann equivalent in G.
- By Perlis' theorem, K, K' are arithmetically equivalent.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- It is given that $\Gamma(\pi_{\sigma_{\mathfrak{Q}}}) = \Gamma(\pi'_{\sigma_{\mathfrak{Q}}})$.
- Take $\omega \in G$.
- By Chebotarev Density Theorem, there exists a prime p unramified in N, and a prime $\mathfrak{Q}$ of N lying over p with $\sigma_{\mathfrak{Q}} = \omega$.
- So $\Gamma(\pi_\omega) = \Gamma(\pi'_\omega)$.
- ω is an arbitrary.
- H and H' are Gassmann equivalent in G.
- By Perlis' theorem, K, K' are arithmetically equivalent.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- It is given that $\Gamma(\pi_{\sigma_{\mathfrak{Q}}}) = \Gamma(\pi'_{\sigma_{\mathfrak{Q}}})$.
- Take $\omega \in G$.
- By Chebotarev Density Theorem, there exists a prime p unramified in N, and a prime $\mathfrak{Q}$ of N lying over p with $\sigma_{\mathfrak{Q}} = \omega$.
- So $\Gamma(\pi_\omega) = \Gamma(\pi'_\omega)$.
- ω is an arbitrary.
- H and H' are Gassmann equivalent in G.
- By Perlis' theorem, K, K' are arithmetically equivalent.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- It is given that $\Gamma(\pi_{\sigma_{\mathfrak{Q}}}) = \Gamma(\pi'_{\sigma_{\mathfrak{Q}}})$.
- Take $\omega \in G$.
- By Chebotarev Density Theorem, there exists a prime p unramified in N, and a prime $\mathfrak{Q}$ of N lying over p with $\sigma_{\mathfrak{Q}} = \omega$.
- So $\Gamma(\pi_\omega) = \Gamma(\pi'_\omega)$.
- ω is an arbitrary.
- H and H' are Gassmann equivalent in G.
- By Perlis' theorem, K, K' are arithmetically equivalent.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- It is given that $\Gamma(\pi_{\sigma_{\mathfrak{Q}}}) = \Gamma(\pi'_{\sigma_{\mathfrak{Q}}})$.
- Take $\omega \in G$.
- By Chebotarev Density Theorem, there exists a prime p unramified in N, and a prime $\mathfrak{Q}$ of N lying over p with $\sigma_{\mathfrak{Q}} = \omega$.
- So $\Gamma(\pi_\omega) = \Gamma(\pi'_\omega)$.
- ω is an arbitrary.
- H and H' are Gassmann equivalent in G.
- By Perlis' theorem, K, K' are arithmetically equivalent.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- It is given that $\Gamma(\pi_{\sigma_{\mathfrak{Q}}}) = \Gamma(\pi'_{\sigma_{\mathfrak{Q}}})$.
- Take $\omega \in G$.
- By Chebotarev Density Theorem, there exists a prime p unramified in N, and a prime $\mathfrak{Q}$ of N lying over p with $\sigma_{\mathfrak{Q}} = \omega$.
- So $\Gamma(\pi_{\omega}) = \Gamma(\pi'_{\omega})$.
- ω is an arbitrary.
- H and H' are Gassmann equivalent in G.
- By Perlis' theorem, K, K' are arithmetically equivalent.

A New Proof Stuart-Perlis Theorem

Proof (cont.)

- It is given that $\Gamma(\pi_{\sigma_{\mathfrak{Q}}}) = \Gamma(\pi'_{\sigma_{\mathfrak{Q}}})$.
- Take $\omega \in G$.
- By Chebotarev Density Theorem, there exists a prime p unramified in N, and a prime $\mathfrak{Q}$ of N lying over p with $\sigma_{\mathfrak{Q}} = \omega$.
- So $\Gamma(\pi_\omega) = \Gamma(\pi'_\omega)$.
- ω is an arbitrary.
- H and H' are Gassmann equivalent in G.
- By Perlis' theorem, K, K' are arithmetically equivalent.

□

A Construction

Theorem

For every natural number n, there exist $n+1$ *arithmetically equivalent number fields* $K_0, K_1, \cdots, K_n$ *such that* K_i *is not isomorphic to* K_j *for* $i \neq j$ *wherel* $i, j = 0, 1, \cdots, n$.

Definition of a Pell Equation

Definition

A *Pell equation* is an equation of the form

$$x^2 - Dy^2 = K,$$

where D is a nonsquare positive integer and K is a nonzero integer.

A Quick History

Question

Why is it called a Pell equation?

It is named after John Pell (1610-1685). There is no evidence that he had ever considered solving such equations.

Lenstra (2002) wrote that *Euler (1707-1783) mistakenly attributed to Pell a solution method that had in fact been found by another mathematician, William Brouncker (1601-1665).*

A Quick History

Question

Why is it called a Pell equation?

It is named after John Pell (1610-1685). There is no evidence that he had ever considered solving such equations.

Lenstra (2002) wrote that *Euler (1707-1783) mistakenly attributed to Pell a solution method that had in fact been found by another mathematician, William Brouncker (1601-1665).*

A Quick History

Question

Why is it called a Pell equation?

It is named after John Pell (1610-1685). There is no evidence that he had ever considered solving such equations.

Lenstra (2002) wrote that *Euler (1707-1783) mistakenly attributed to Pell a solution method that had in fact been found by another mathematician, William Brouncker (1601-1665).*

The more common Pell equations studied are

$$x^2 - Dy^2 = \pm 1,$$

$$x^2 - Dy^2 = \pm 2,$$

$$x^2 - Dy^2 = \pm 4,$$

where D is a nonsquare integer.

How can one solve the equation

$$x^2 - Dy^2 = 1?$$

The more common Pell equations studied are

$$x^2 - Dy^2 = \pm 1,$$

$$x^2 - Dy^2 = \pm 2,$$

$$x^2 - Dy^2 = \pm 4,$$

where D is a nonsquare integer.

How can one solve the equation

$$x^2 - Dy^2 = 1?$$

Let us consider all solutions $x + y\sqrt{D}$ of the equation

$$x^2 - Dy^2 = 1,$$

with positive x and y.

Among these solutions, there is a least solution $x_1 + y_1\sqrt{D}$, in which x_1 and y_1 have their least positive values. The number $x_1 + y_1\sqrt{D}$ is called the *fundamental solution* of the Pell equation.

Let us consider all solutions $x + y\sqrt{D}$ of the equation

$$x^2 - Dy^2 = 1,$$

with positive x and y.

Among these solutions, there is a least solution $x_1 + y_1\sqrt{D}$, in which x_1 and y_1 have their least positive values. The number $x_1 + y_1\sqrt{D}$ is called the *fundamental solution* of the Pell equation.

Theorem 104, Nagell

Theorem

If D is a natural number which is not a perfect square, the Pell equation

$$x^2 - Dy^2 = 1$$

has infinitely many solutions $x + y\sqrt{D}$. All solutions with positive x_n and y_n are obtained by the formula

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n,$$

where $x_1 + y_1\sqrt{D}$ is the fundamental of the Pell equation.

Examples

Example

The fundamental solution of $x^2 - 2y^2 = 1$ is

$$3 + 2\sqrt{2}.$$

Upto sign, all the positive integer solutions are given by

$$(x + y\sqrt{2}) = (3 + 2\sqrt{2})^n,$$

with $n \geq 1$.

Theorem (Dossavi-Yovo, Luca, Togbe (2015))

Let $d \geq 2$ be square-free. The Diophantine equation

$$x_n = a\left(\frac{10^m - 1}{9}\right), \qquad m \geq 1 \text{ and } a \in \{1, \ldots, 9\} \tag{2}$$

has at most one positive integer solution n with the following exceptions:

1. $d = 2$, $n \in \{1, 3\}$;
2. $d = 3$, $n \in \{1, 2\}$.

Theorem (Faye, Luca (2015))

Let $b \geq 2$ be fixed. Let $d \geq 2$ be squarefree et let $(x_n, y_n) = (x_n(d), y_n(d))$ be the nth positive integer solution of the Pell equation $x^2 - dy^2 = 1$. If the Diophantine equation

$$x_n = a\left(\frac{b^m - 1}{b - 1}\right), \qquad m \geq 1 \text{ and } a \in \{1, \ldots, b-1\} \tag{3}$$

has two positive integer solutions (n, a, m), then

$$d \leq \exp\left((10b)^{10^5}\right).$$

Let $d \geq 2$ be an integer which is not a square. Now, we consider the Pell equation

$$x^2 - dy^2 = \pm 4. \tag{4}$$

Before getting to our main result, let us make some numerical observations. It is known that all positive integer solutions (x, y) of (4) are given by

$$\frac{x_n + y_n\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^n$$

for some positive integer n, where (x_1, y_1) is the smallest positive integer solution.

Let $\{F_m\}_{m\geq 0}$ be the Fibonacci sequence.

We study when can x_n be a Fibonacci number, which reduces to the Diophantine equation

$$x_n \in \{F_m\}_{m\geq 1}. \tag{5}$$

- If $m = 1, 2$, then $x_n = F_m = 1$. Using equation (4), we get that $n = 1, d = 5, Y_n = 1$.
- If $m = 3$, then $x_n = F_m = 2$. Using equation (4), we get that $n = 1, d = 2, y_n = 2$.

Let $\{F_m\}_{m\geq 0}$ be the Fibonacci sequence.

We study when can x_n be a Fibonacci number, which reduces to the Diophantine equation

$$x_n \in \{F_m\}_{m\geq 1}. \tag{5}$$

- If $m = 1, 2$, then $x_n = F_m = 1$. Using equation (4), we get that $n = 1$, $d = 5$, $Y_n = 1$.
- If $m = 3$, then $x_n = F_m = 2$. Using equation (4), we get that $n = 1$, $d = 2$, $y_n = 2$.

Theorem (K., Luca, Togbe (2016))

Let $d \geq 2$ be a square-free integer. The Diophantine equation

$$x_n \in \{F_m\}_{m \geq 4} \tag{6}$$

has at most one solution (n, m) in positive integers. Allowing also $m \in \{1, 2, 3\}$, the above Diophantine equation still has at most one solution except for $d = 2$ and $d = 5$, cases in which

$$n \in \{1, 4\}, \quad \textit{and} \quad n \in \{1, 2\},$$

respectively, are all the solutions of the containment (6).

The proof is made in two parts.

Theorem (K., Luca, Togbe (2016))

Let $d \geq 2$ be a square-free integer. The Diophantine equation

$$x_n \in \{F_m\}_{m \geq 4} \tag{6}$$

has at most one solution (n, m) in positive integers. Allowing also $m \in \{1, 2, 3\}$, the above Diophantine equation still has at most one solution except for $d = 2$ and $d = 5$, cases in which

$$n \in \{1, 4\}, \quad \textit{and} \quad n \in \{1, 2\},$$

respectively, are all the solutions of the containment (6).

The proof is made in two parts.

First Part: n is even

Write $n = 2n_1$. Since

$$x_n = x_{2n_1} = x_{n_1}^2 - 2\epsilon, \text{ with } \epsilon \in \{\pm 1\}.$$

Therefore, it suffices to solve the equation

$$x^2 \pm 2 = F_m, \text{ where } m \geq 1.$$

We obtain four elliptic curves of the form

$$v^2 = 5(u^2 \pm 2)^2 \pm 4.$$

We obtained only one acceptable solution $(u, v) = (2, 16)$, leading us $x_n = F_m = 2 = F_3$, and $y_n = 2$.

First Part: n is even

Write $n = 2n_1$. Since

$$x_n = x_{2n_1} = x_{n_1}^2 - 2\epsilon, \text{ with } \epsilon \in \{\pm 1\}.$$

Therefore, it suffices to solve the equation

$$x^2 \pm 2 = F_m, \text{ where } m \geq 1.$$

We obtain four elliptic curves of the form

$$v^2 = 5(u^2 \pm 2)^2 \pm 4.$$

We obtained only one acceptable solution $(u, v) = (2, 16)$, leading us $x_n = F_m = 2 = F_3$, and $y_n = 2$.

First Part: n is even

Write $n = 2n_1$. Since

$$x_n = x_{2n_1} = x_{n_1}^2 - 2\epsilon, \text{ with } \epsilon \in \{\pm 1\}.$$

Therefore, it suffices to solve the equation

$$x^2 \pm 2 = F_m, \text{ where } m \geq 1.$$

We obtain four elliptic curves of the form

$$v^2 = 5(u^2 \pm 2)^2 \pm 4.$$

We obtained only one acceptable solution $(u, v) = (2, 16)$, leading us $x_n = F_m = 2 = F_3$, and $y_n = 2$.

Lemma

Assume that $X^2 - dY^2 = \pm 4$ and that $X_n = F_m$ for some even n. Then, $(n, d) = (2, 5),\ (4, 2)$. Additionally, if $d = 2$ and $d = 5$, the only solutions of $X_n = F_m$ are $n = 1, 4$, and $n = 1, 2$, respectively.

Second Part: n is odd

With some simple observations, we set

$$x_1 = F_{m_1} \text{ and } x_n = F_{m_1 t},$$

where m_1, t are positive integeres > 1.

We consider several techniques to bound the parameters m_1, n.

- $\gamma^{m_1} < 6n^2$, where $\gamma = \dfrac{1+\sqrt{5}}{2}$.
- Then, we use a Baker's method (Matveev version) to get $n \leq 2.9 \times 10^{15}$, and $m_1 \leq 154$.
- To consider the remaining cases, for $m_1 \in [4, 154]$, we use the Baker-Davenport reduction method , which gives us $n < m_1 t \leq 157$.

Second Part: n is odd

With some simple observations, we set

$$x_1 = F_{m_1} \text{ and } x_n = F_{m_1 t},$$

where m_1, t are positive integeres > 1.

We consider several techniques to bound the parameters m_1, n.

- $\gamma^{m_1} < 6n^2$, where $\gamma = \frac{1+\sqrt{5}}{2}$.
- Then, we use a Baker's method (Matveev version) to get $n \leq 2.9 \times 10^{15}$, and $m_1 \leq 154$.
- To consider the remaining cases, for $m_1 \in [4, 154]$, we use the Baker-Davenport reduction method , which gives us $n < m_1 t \leq 157$.

Thank You!