Adventures in Binary Quadratic Forms

or: What I Did over Winter Break

Vadim Ponomarenko

Department of Mathematics and Statistics
San Diego State University

University of California at Irvine May 24, 2018

http://vadim.sdsu.edu/2018-UCI-talk.pdf

SAN DIEGO STATE UNIVERSITY

Shameless advertising

Please encourage your students to apply to the
San Diego State University Mathematics REU.

Serious projects.

`http://www.sci.sdsu.edu/math-reu/index.html`

This not-so-serious work had major contributions from Jackson Autry, and minor contributions from J.T. Dimabayao and O.J.Q. Tigas.

San Diego State University

Shameless advertising

Please encourage your students to apply to the San Diego State University Mathematics REU.

Serious projects.

`http://www.sci.sdsu.edu/math-reu/index.html`

This not-so-serious work had major contributions from Jackson Autry, and minor contributions from J.T. Dimabayao and O.J.Q. Tigas.

The Problem to be Solved

Two weeks off for winter break, want palate cleanser.

No time for heavy reading:

A Challenge Appears

"A note on primes of the form $a^2 \pm ab + 2b^2$", Dimabayao and Tigas – declined

"Prime numbers p with expression $p = a^2 \pm ab \pm b^2$", Bahmanpour, Journal of Number Theory 166 (2016) 208-218.

Amazing! OK...

A Challenge Appears

"A note on primes of the form $a^2 \pm ab + 2b^2$", Dimabayao and Tigas – declined

"Prime numbers p with expression $p = a^2 \pm ab \pm b^2$", Bahmanpour, Journal of Number Theory 166 (2016) 208-218.

Amazing! OK...

A Challenge Appears

"A note on primes of the form $a^2 \pm ab + 2b^2$", Dimabayao and Tigas – declined

"Prime numbers p with expression $p = a^2 \pm ab \pm b^2$", Bahmanpour, Journal of Number Theory 166 (2016) 208-218.

Amazing! OK…

My Entry Point

Integers represented by quadratic Form $x^2 + y^2$:

1. [Fermat 1640] Prime p is represented by $x^2 + y^2$ iff $p = 2$ or $p \equiv 1 \pmod 4$.
2. [Girard 1625] Natural n is represented by $x^2 + y^2$ iff every prime dividing n that is congruent to $3 \pmod 4$, appears to an even power.

Irreducibles in (multiplicative) monoid are: “good” primes $(2, 5, 13, \ldots)$, squares of “bad” primes $(3^2, 7^2, 11^2, \ldots)$.

Monoids and irreducibles make Vadim happy.

My Entry Point

Integers represented by quadratic Form $x^2 + y^2$:

1. [Fermat 1640] Prime p is represented by $x^2 + y^2$ iff $p = 2$ or $p \equiv 1 \pmod 4$.
2. [Girard 1625] Natural n is represented by $x^2 + y^2$ iff every prime dividing n that is congruent to $3 \pmod 4$, appears to an even power.

Irreducibles in (multiplicative) monoid are: “good” primes $(2, 5, 13, \ldots)$, squares of “bad” primes $(3^2, 7^2, 11^2, \ldots)$.

Monoids and irreducibles make Vadim happy.

My Entry Point

Integers represented by quadratic Form $x^2 + y^2$:

1. [Fermat 1640] Prime p is represented by $x^2 + y^2$ iff $p = 2$ or $p \equiv 1 \pmod 4$.
2. [Girard 1625] Natural n is represented by $x^2 + y^2$ iff every prime dividing n that is congruent to $3 \pmod 4$, appears to an even power.

Irreducibles in (multiplicative) monoid are: "good" primes $(2, 5, 13, \ldots)$, squares of "bad" primes $(3^2, 7^2, 11^2, \ldots)$.

Monoids and irreducibles make Vadim happy.

Recent Work

1. [Bahmanpour 2016] Prime p is represented by $x^2 + xy - y^2$ iff $p \equiv 0, 1, -1 \pmod 5$. Prime p is represented by $x^2 + xy + y^2$ iff $p \equiv 0, 1 \pmod 3$.
2. [Nair arxiv:2004] Natural n is represented by $x^2 + xy + y^2$ iff every prime dividing n that is congruent to $2 \pmod 3$, appears to an even power.

Monoids and irreducibles again...?

Recent Work

1. [Bahmanpour 2016] Prime p is represented by $x^2 + xy - y^2$ iff $p \equiv 0, 1, -1 \pmod 5$. Prime p is represented by $x^2 + xy + y^2$ iff $p \equiv 0, 1 \pmod 3$.
2. [Nair arxiv:2004] Natural n is represented by $x^2 + xy + y^2$ iff every prime dividing n that is congruent to $2 \pmod 3$, appears to an even power.

Monoids and irreducibles again...?

Recent Work

1. [Bahmanpour 2016] Prime p is represented by $x^2 + xy - y^2$ iff $p \equiv 0, 1, -1 \pmod 5$. Prime p is represented by $x^2 + xy + y^2$ iff $p \equiv 0, 1 \pmod 3$.
2. [Nair arxiv:2004] Natural n is represented by $x^2 + xy + y^2$ iff every prime dividing n that is congruent to $2 \pmod 3$, appears to an even power.

Monoids and irreducibles again...?

My Other Background

1. [Pell's equation] 1 is represented by $x^2 - ny^2$, provided n is a nonsquare (Lagrange).
2. [negative Pell's equation] -1 is represented by $x^2 - ny^2$, provided continued fractions...
3. Quadratic fields...
4. Quadratic forms...

Damn the torpedoes, time to prove something (original or not).

San Diego State University

My Other Background

1. [Pell's equation] 1 is represented by $x^2 - ny^2$, provided n is a nonsquare (Lagrange).
2. [negative Pell's equation] -1 is represented by $x^2 - ny^2$, provided continued fractions...
3. Quadratic fields...
4. Quadratic forms...

Damn the torpedoes, time to prove something (original or not).

My Other Background

1. [Pell's equation] 1 is represented by $x^2 - ny^2$, provided n is a nonsquare (Lagrange).
2. [negative Pell's equation] -1 is represented by $x^2 - ny^2$, provided continued fractions...
3. Quadratic fields...
4. Quadratic forms...

Damn the torpedoes, time to prove something (original or not).

My Other Background

1. [Pell's equation] 1 is represented by $x^2 - ny^2$, provided n is a nonsquare (Lagrange).
2. [negative Pell's equation] -1 is represented by $x^2 - ny^2$, provided continued fractions...
3. Quadratic fields...
4. Quadratic forms...

Damn the torpedoes, time to prove something (original or not).

My Other Background

1. [Pell's equation] 1 is represented by $x^2 - ny^2$, provided n is a nonsquare (Lagrange).
2. [negative Pell's equation] -1 is represented by $x^2 - ny^2$, provided continued fractions...
3. Quadratic fields...
4. Quadratic forms...

Damn the torpedoes, time to prove something (original or not).

SAN DIEGO STATE UNIVERSITY

Outline

1. What was known going in. (complete)
2. What was proved.
3. What was learned afterward.
4. What will happen next.

"New" Result

Given a principal binary quadratic form $x^2 + xy + ny^2$,

with $\tau = |1 - 4n|$ prime,

if Condition P holds,

then a full characterization of which integers are represented is provided.

Note 1: $n = 1$ gives $\tau = 3$, $n = -1$ gives $\tau = 5$.
Note 2: Condition P fairly easy to test computationally.
Note 3: Generalizes to $x^2 + mxy + ny^2$, with prime $|m^2 - 4n|$.

SAN DIEGO STATE UNIVERSITY

"New" Result

Given a principal binary quadratic form $x^2 + xy + ny^2$,

with $\tau = |1 - 4n|$ prime,

if Condition P holds,

then a full characterization of which integers are represented is provided.

Note 1: $n = 1$ gives $\tau = 3$, $n = -1$ gives $\tau = 5$.
Note 2: Condition P fairly easy to test computationally.
Note 3: Generalizes to $x^2 + mxy + ny^2$, with prime $|m^2 - 4n|$.

"New" Result

Given a principal binary quadratic form $x^2 + xy + ny^2$,

with $\tau = |1 - 4n|$ prime,

if Condition P holds,

then a full characterization of which integers are represented is provided.

Note 1: $n = 1$ gives $\tau = 3$, $n = -1$ gives $\tau = 5$.
Note 2: Condition P fairly easy to test computationally.
Note 3: Generalizes to $x^2 + mxy + ny^2$, with prime $|m^2 - 4n|$.

"New" Result

Given a principal binary quadratic form $x^2 + xy + ny^2$,

with $\tau = |1 - 4n|$ prime,

if Condition P holds,

then a full characterization of which integers are represented is provided.

Note 1: $n = 1$ gives $\tau = 3$, $n = -1$ gives $\tau = 5$.
Note 2: Condition P fairly easy to test computationally.
Note 3: Generalizes to $x^2 + mxy + ny^2$, with prime $|m^2 - 4n|$.

"New" Result

Given a principal binary quadratic form $x^2 + xy + ny^2$,

with $\tau = |1 - 4n|$ prime,

if Condition P holds,

then a full characterization of which integers are represented is provided.

Note 1: $n = 1$ gives $\tau = 3$, $n = -1$ gives $\tau = 5$.
Note 2: Condition P fairly easy to test computationally.
Note 3: Generalizes to $x^2 + mxy + ny^2$, with prime $|m^2 - 4n|$.

“New” Result

Given a principal binary quadratic form $x^2 + xy + ny^2$,

with $\tau = |1 - 4n|$ prime,

if Condition P holds,

then a full characterization of which integers are represented is provided.

Note 1: $n = 1$ gives $\tau = 3$, $n = -1$ gives $\tau = 5$.
Note 2: Condition P fairly easy to test computationally.
Note 3: Generalizes to $x^2 + mxy + ny^2$, with prime $|m^2 - 4n|$.

“New” Result

Given a principal binary quadratic form $x^2 + xy + ny^2$,

with $\tau = |1 - 4n|$ prime,

if Condition P holds,

then a full characterization of which integers are represented is provided.

Note 1: $n = 1$ gives $\tau = 3$, $n = -1$ gives $\tau = 5$.
Note 2: Condition P fairly easy to test computationally.
Note 3: Generalizes to $x^2 + mxy + ny^2$, with prime $|m^2 - 4n|$.

A look at τ

Given $x^2 + xy + ny^2$, set $\tau = |1 - 4n|$. Discriminant $\Delta = 1 - 4n$.

If $n > 0$, then $\Delta < 0$ and $\tau \equiv 3 \pmod 4$. “positive definite qf”

If $n < 0$, then $\Delta > 0$ and $\tau \equiv 1 \pmod 4$. “indefinite qf”

In both cases, $\Delta \equiv 1 \pmod 4$, since τ is assumed prime.

A look at τ

Given $x^2 + xy + ny^2$, set $\tau = |1 - 4n|$. Discriminant $\Delta = 1 - 4n$.

If $n > 0$, then $\Delta < 0$ and $\tau \equiv 3 \pmod 4$. "positive definite qf"

If $n < 0$, then $\Delta > 0$ and $\tau \equiv 1 \pmod 4$. "indefinite qf"

In both cases, $\Delta \equiv 1 \pmod 4$, since τ is assumed prime.

Where's the monoid?

Set $K_n = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}\} \subseteq \mathbb{Z}$.

$$(a^2 + ab + nb^2)(c^2 + cd + nd^2) =$$
$$(\underbrace{ac - nbd}_{e})^2 + (\underbrace{ac - nbd}_{e})(\underbrace{bc + ad + bd}_{f}) + n(\underbrace{bc + ad + bd}_{f})^2$$

$1 = 1^2 + 1 \cdot 0 + n(0)^2$ Monoid!

Set $K_n' = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\} \subseteq K_n$

Note that if $p \in K_n$ is prime, then in fact $p \in K_n'$.

San Diego State University

Where's the monoid?

Set $K_n = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}\} \subseteq \mathbb{Z}$.

$$(a^2 + ab + nb^2)(c^2 + cd + nd^2) =$$
$$(\underbrace{ac - nbd}_{e})^2 + (\underbrace{ac - nbd}_{e})(\underbrace{bc + ad + bd}_{f}) + n(\underbrace{bc + ad + bd}_{f})^2$$

$1 = 1^2 + 1 \cdot 0 + n(0)^2$ Monoid!

Set $K_n' = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\} \subseteq K_n$

Note that if $p \in K_n$ is prime, then in fact $p \in K_n'$.

Where's the monoid?

Set $K_n = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}\} \subseteq \mathbb{Z}$.

$$(a^2 + ab + nb^2)(c^2 + cd + nd^2) =$$
$$(\underbrace{ac - nbd}_{e})^2 + (\underbrace{ac - nbd}_{e})(\underbrace{bc + ad + bd}_{f}) + n(\underbrace{bc + ad + bd}_{f})^2$$

$1 = 1^2 + 1 \cdot 0 + n(0)^2$ Monoid!

Set $K_n' = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\} \subseteq K_n$

Note that if $p \in K_n$ is prime, then in fact $p \in K_n'$.

Where's the monoid?

Set $K_n = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}\} \subseteq \mathbb{Z}$.

$$(a^2 + ab + nb^2)(c^2 + cd + nd^2) =$$
$$(\underbrace{ac - nbd}_{e})^2 + (\underbrace{ac - nbd}_{e})(\underbrace{bc + ad + bd}_{f}) + n(\underbrace{bc + ad + bd}_{f})^2$$

$1 = 1^2 + 1 \cdot 0 + n(0)^2$ Monoid!

Set $K'_n = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\} \subseteq K_n$

Note that if $p \in K_n$ is prime, then in fact $p \in K'_n$.

K_n for $n < 0$

Recall: $x^2 + xy + ny^2$. If $n < 0$ then $\tau = |1 - 4n| = 1 - 4n$.

Lemma: Let $n < 0$. Then $-1 \in K_n$.
Proof: $\tau \equiv 1 \pmod 4$ is prime, so negative Pell equation $x^2 - \tau y^2 = -1$ has a solution. We see that
$(-x - y)^2 + (-x - y)(2y) + n(2y)^2 = x^2 - (1 - 4n)y^2 = -1.$

Corollary: $K_n = -K_n$

SAN DIEGO STATE UNIVERSITY

K_n for $n < 0$

Recall: $x^2 + xy + ny^2$. If $n < 0$ then $\tau = |1 - 4n| = 1 - 4n$.

Lemma: Let $n < 0$. Then $-1 \in K_n$.
Proof: $\tau \equiv 1 \pmod 4$ is prime, so negative Pell equation $x^2 - \tau y^2 = -1$ has a solution. We see that
$(-x - y)^2 + (-x - y)(2y) + n(2y)^2 = x^2 - (1 - 4n)y^2 = -1$.

Corollary: $K_n = -K_n$

K_n for $n < 0$

Recall: $x^2 + xy + ny^2$. If $n < 0$ then $\tau = |1 - 4n| = 1 - 4n$.

Lemma: Let $n < 0$. Then $-1 \in K_n$.
Proof: $\tau \equiv 1 \pmod 4$ is prime, so negative Pell equation $x^2 - \tau y^2 = -1$ has a solution. We see that
$(-x-y)^2 + (-x-y)(2y) + n(2y)^2 = x^2 - (1-4n)y^2 = -1$.

Corollary: $K_n = -K_n$

K_n for $n > 0$

Recall: $x^2 + xy + ny^2$. If $n > 0$ then $\tau = |1 - 4n| = 4n - 1 > 0$.

Lemma: Let $n > 0$. Then $K_n \subseteq \mathbb{N}_0$.
Proof: Let $a, b \in \mathbb{Z}$. Set $s = n^{-1/2}, b' = bn^{1/2}$. Note: $b = sb'$.
$a^2 + ab + nb^2 = a^2 + sab' + (b')^2 = \frac{2+s}{4}(a + b')^2 + \frac{2-s}{4}(a - b')^2$.
Now $|s| < 2$, so $\frac{2 \pm s}{4} > 0$. Hence $a^2 + ab + nb^2 \geq 0$, with equality iff $a = b = 0$.

Representing τ and squares

Recall: $x^2 + xy + ny^2$. $\tau = |1 - 4n|$ is assumed prime.

Lemma: $\tau \in K_n$.
Proof: $(-1)^2 + (-1)(2) + n(2)^2 = -1 + 4n$. For $n > 0$, this is τ.
For $n < 0$, this is $-\tau$, but $K_n = -K_n$.

Lemma: For any $x \in \mathbb{N}$, $x^2 \in K_n$.
Proof: $x^2 + x(0) + n(0)^2$.

Representing τ and squares

Recall: $x^2 + xy + ny^2$. $\tau = |1 - 4n|$ is assumed prime.

Lemma: $\tau \in K_n$.
Proof: $(-1)^2 + (-1)(2) + n(2)^2 = -1 + 4n$. For $n > 0$, this is τ.
For $n < 0$, this is $-\tau$, but $K_n = -K_n$.

Lemma: For any $x \in \mathbb{N}$, $x^2 \in K_n$.
Proof: $x^2 + x(0) + n(0)^2$.

Representing nonresidues

Recall: $x^2 + xy + ny^2$. $\tau = |1 - 4n|$ is assumed prime.

Lemma: If $t \neq \tau$ is a quadratic nonresidue mod τ, then $t \notin K_n$.
Proof: ABWOC, $t = a^2 + ab + nb^2$. Working mod τ,
$4t \equiv 4a^2 + 4ab + 4nb^2 \equiv (2a+b)^2 + b^2(4n-1) \equiv (2a+b)^2$.
Hence $1 = \left(\frac{4t}{\tau}\right) = \left(\frac{t}{\tau}\right)\left(\frac{2}{\tau}\right)^2 = \left(\frac{t}{\tau}\right) = -1$, a contradiction.

Prime τ: yes
Nonresidues: no
Residues: ?

Representing nonresidues

Recall: $x^2 + xy + ny^2$. $\tau = |1 - 4n|$ is assumed prime.

Lemma: If $t \neq \tau$ is a quadratic nonresidue mod τ, then $t \notin K_n$.
Proof: ABWOC, $t = a^2 + ab + nb^2$. Working mod τ,
$4t \equiv 4a^2 + 4ab + 4nb^2 \equiv (2a+b)^2 + b^2(4n-1) \equiv (2a+b)^2$.
Hence $1 = \left(\frac{4t}{\tau}\right) = \left(\frac{t}{\tau}\right)\left(\frac{2}{\tau}\right)^2 = \left(\frac{t}{\tau}\right) = -1$, a contradiction.

Prime τ: yes
Nonresidues: no
Residues: ?

Representing nonresidues

Recall: $x^2 + xy + ny^2$. $\tau = |1 - 4n|$ is assumed prime.

Lemma: If $t \neq \tau$ is a quadratic nonresidue mod τ, then $t \notin K_n$.
Proof: ABWOC, $t = a^2 + ab + nb^2$. Working mod τ,
$4t \equiv 4a^2 + 4ab + 4nb^2 \equiv (2a+b)^2 + b^2(4n-1) \equiv (2a+b)^2$.
Hence $1 = \left(\frac{4t}{\tau}\right) = \left(\frac{t}{\tau}\right)\left(\frac{2}{\tau}\right)^2 = \left(\frac{t}{\tau}\right) = -1$, a contradiction.

Prime τ: yes
Nonresidues: no
Residues: ?

Quadratic Reciprocity

Recall: $x^2 + xy + ny^2$. $\tau = |1 - 4n|$ is assumed prime.

Lemma: Let $p \neq \tau$ be an odd prime. Then $\left(\frac{p}{\tau}\right) = \left(\frac{1-4n}{p}\right)$.

Proof: If $n < 0$, then $\tau = 1 - 4n$ and $\tau \equiv 1 \pmod 4$, so by quadratic reciprocity $\left(\frac{p}{\tau}\right) = \left(\frac{\tau}{p}\right) = \left(\frac{1-4n}{p}\right)$.

If $n > 0$, then $\tau = 4n - 1$ and $\tau \equiv 3 \pmod 4$, so by QR $(-1)^{(p-1)/2} = \left(\frac{p}{\tau}\right)\left(\frac{\tau}{p}\right) = \left(\frac{p}{\tau}\right)\left(\frac{1-4n}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{p}{\tau}\right)\left(\frac{1-4n}{p}\right)(-1)^{(p-1)/2}$.

Quadratic Reciprocity

Recall: $x^2 + xy + ny^2$. $\tau = |1 - 4n|$ is assumed prime.

Lemma: Let $p \neq \tau$ be an odd prime. Then $\left(\frac{p}{\tau}\right) = \left(\frac{1-4n}{p}\right)$.

Proof: If $n < 0$, then $\tau = 1 - 4n$ and $\tau \equiv 1 \pmod 4$, so by quadratic reciprocity $\left(\frac{p}{\tau}\right) = \left(\frac{\tau}{p}\right) = \left(\frac{1-4n}{p}\right)$.

If $n > 0$, then $\tau = 4n - 1$ and $\tau \equiv 3 \pmod 4$, so by QR $(-1)^{(p-1)/2} = \left(\frac{p}{\tau}\right)\left(\frac{\tau}{p}\right) = \left(\frac{p}{\tau}\right)\left(\frac{1-4n}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{p}{\tau}\right)\left(\frac{1-4n}{p}\right)(-1)^{(p-1)/2}$.

Quadratic Reciprocity

Recall: $x^2 + xy + ny^2$. $\tau = |1 - 4n|$ is assumed prime.

Lemma: Let $p \neq \tau$ be an odd prime. Then $\left(\frac{p}{\tau}\right) = \left(\frac{1-4n}{p}\right)$.

Proof: If $n < 0$, then $\tau = 1 - 4n$ and $\tau \equiv 1 \pmod 4$, so by quadratic reciprocity $\left(\frac{p}{\tau}\right) = \left(\frac{\tau}{p}\right) = \left(\frac{1-4n}{p}\right)$.

If $n > 0$, then $\tau = 4n - 1$ and $\tau \equiv 3 \pmod 4$, so by QR $(-1)^{(p-1)/2} = \left(\frac{p}{\tau}\right)\left(\frac{\tau}{p}\right) = \left(\frac{p}{\tau}\right)\left(\frac{1-4n}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{p}{\tau}\right)\left(\frac{1-4n}{p}\right)(-1)^{(p-1)/2}$.

Key Lemma

Recall: $K'_n = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\} \subseteq K_n$

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K'_n$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Proof: By QR lemma, there is $r \in \mathbb{Z}$ with $r^2 \equiv 1 - 4n \pmod{p}$. Take s with $2s + 1 \equiv r \pmod{p}$. $4s^2 + 4s + 4n \equiv 0 \pmod{p}$, so $s^2 + s + n \equiv 0 \pmod{p}$. Hence there is t' with $t'p \in K'_n$.

Take $g(x) = (s + xp)^2 + (s + xp) + n$. If $x \in \mathbb{Z}$, then $p|g(x)$. Vertex is $k' = -\frac{2s+1}{2p}$. $g(k') = \frac{4n-1}{4}$, $g(k' \pm \frac{1}{2}) = \frac{4n-1}{4} + \frac{p^2}{4}$. Take integer $k \in [k' - \frac{1}{2}, k' + \frac{1}{2}]$. So $p|g(k)$, and $g(k) \in [\frac{4n-1}{4}, \frac{4n-1}{4} + \frac{p^2}{4}]$. $|g(k)| \leq \frac{\tau}{4} + \frac{p^2}{4} < \frac{3p^2}{4} + \frac{p^2}{4} = p^2$. So $g(k) = pt$ with $|t| < p$. $|t| > 0$ since $0 \notin K'_n$ (IOU).

San Diego State University

Key Lemma

Recall: $K_n' = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\} \subseteq K_n$

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Proof: By QR lemma, there is $r \in \mathbb{Z}$ with $r^2 \equiv 1 - 4n \pmod{p}$. Take s with $2s + 1 \equiv r \pmod{p}$. $4s^2 + 4s + 4n \equiv 0 \pmod{p}$, so $s^2 + s + n \equiv 0 \pmod{p}$. Hence there is t' with $t'p \in K_n'$.

Take $g(x) = (s + xp)^2 + (s + xp) + n$. If $x \in \mathbb{Z}$, then $p|g(x)$. Vertex is $k' = -\frac{2s+1}{2p}$. $g(k') = \frac{4n-1}{4}$, $g(k' \pm \frac{1}{2}) = \frac{4n-1}{4} + \frac{p^2}{4}$. Take integer $k \in [k' - \frac{1}{2}, k' + \frac{1}{2}]$. So $p|g(k)$, and $g(k) \in [\frac{4n-1}{4}, \frac{4n-1}{4} + \frac{p^2}{4}]$. $|g(k)| \leq \frac{\tau}{4} + \frac{p^2}{4} < \frac{3p^2}{4} + \frac{p^2}{4} = p^2$. So $g(k) = pt$ with $|t| < p$. $|t| > 0$ since $0 \notin K_n'$ (IOU).

San Diego State University

Key Lemma

Recall: $K_n' = \{x^2 + xy + ny^2 : x, y \in \mathbb{Z}, \gcd(x, y) = 1\} \subseteq K_n$

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Proof: By QR lemma, there is $r \in \mathbb{Z}$ with $r^2 \equiv 1 - 4n \pmod{p}$. Take s with $2s + 1 \equiv r \pmod{p}$. $4s^2 + 4s + 4n \equiv 0 \pmod{p}$, so $s^2 + s + n \equiv 0 \pmod{p}$. Hence there is t' with $t'p \in K_n'$.

Take $g(x) = (s + xp)^2 + (s + xp) + n$. If $x \in \mathbb{Z}$, then $p|g(x)$. Vertex is $k' = -\frac{2s+1}{2p}$. $g(k') = \frac{4n-1}{4}$, $g(k' \pm \frac{1}{2}) = \frac{4n-1}{4} + \frac{p^2}{4}$. Take integer $k \in [k' - \frac{1}{2}, k' + \frac{1}{2}]$. So $p|g(k)$, and $g(k) \in [\frac{4n-1}{4}, \frac{4n-1}{4} + \frac{p^2}{4}]$. $|g(k)| \leq \frac{\tau}{4} + \frac{p^2}{4} < \frac{3p^2}{4} + \frac{p^2}{4} = p^2$. So $g(k) = pt$ with $|t| < p$. $|t| > 0$ since $0 \notin K_n'$ (IOU).

SAN DIEGO STATE UNIVERSITY

Main Result Sketch

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Proof: ABWOC, p minimal prime with $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$. Condition P implies $p > \sqrt{\frac{\tau}{3}}$. Applying Key Lemma, choose $|t|$ minimal with $0 < |t| < p$ and $pt \in K_n'$.

$|t| = 1$ impossible. So write $|t| = p_1 p_2 \cdots p_k$, with each p_i prime and $p_i < p$. By (IOU), each $p_i \notin K_n$. By (IOU), each p_i must be 2, and by (IOU), $k \leq 1$. Finally, $t = 2$, but then $pt = 2p$, a nonresidue, so $pt \notin K_n$.

Main Result Sketch

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Proof: ABWOC, p minimal prime with $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$. Condition P implies $p > \sqrt{\frac{\tau}{3}}$. Applying Key Lemma, choose $|t|$ minimal with $0 < |t| < p$ and $pt \in K_n'$.

$|t| = 1$ impossible. So write $|t| = p_1 p_2 \cdots p_k$, with each p_i prime and $p_i < p$. By (IOU), each $p_i \notin K_n$. By (IOU), each p_i must be 2, and by (IOU), $k \leq 1$. Finally, $t = 2$, but then $pt = 2p$, a nonresidue, so $pt \notin K_n$.

Main Result Sketch

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Proof: ABWOC, p minimal prime with $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$. Condition P implies $p > \sqrt{\frac{\tau}{3}}$. Applying Key Lemma, choose $|t|$ minimal with $0 < |t| < p$ and $pt \in K_n'$.

$|t| = 1$ impossible. So write $|t| = p_1 p_2 \cdots p_k$, with each p_i prime and $p_i < p$. By (IOU), each $p_i \notin K_n$. By (IOU), each p_i must be 2, and by (IOU), $k \leq 1$. Finally, $t = 2$, but then $pt = 2p$, a nonresidue, so $pt \notin K_n$.

Condition P

In the theorem, we need $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$ to imply $p > \sqrt{\frac{\tau}{3}}$.

Set $P_\tau = \{p \text{ prime } : \left(\frac{p}{\tau}\right) = 1, p \leq \sqrt{\frac{\tau}{3}}\}$.

Condition P is just: $P_\tau \subseteq K_n$

For $n = \pm 1$, $P_3 = P_5 = \emptyset$, so Condition P holds vacuously.
For $n = -4$, $P_{17} = \{2\}$; we verify condition P via $2 = 2^2 + 2(1) + (-4)(1)^2$.

Lots of computational data available.

Condition P

In the theorem, we need $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$ to imply $p > \sqrt{\frac{\tau}{3}}$.

Set $P_\tau = \{p \text{ prime } : \left(\frac{p}{\tau}\right) = 1, p \leq \sqrt{\frac{\tau}{3}}\}$.
Condition P is just: $P_\tau \subseteq K_n$

For $n = \pm 1$, $P_3 = P_5 = \emptyset$, so Condition P holds vacuously.
For $n = -4$, $P_{17} = \{2\}$; we verify condition P via
$2 = 2^2 + 2(1) + (-4)(1)^2$.

Lots of computational data available.

Condition P

In the theorem, we need $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$ to imply $p > \sqrt{\frac{\tau}{3}}$.

Set $P_\tau = \{p \text{ prime } : \left(\frac{p}{\tau}\right) = 1, p \leq \sqrt{\frac{\tau}{3}}\}$.

Condition P is just: $P_\tau \subseteq K_n$

For $n = \pm 1$, $P_3 = P_5 = \emptyset$, so Condition P holds vacuously.
For $n = -4$, $P_{17} = \{2\}$; we verify condition P via
$2 = 2^2 + 2(1) + (-4)(1)^2$.

Lots of computational data available.

Condition P

In the theorem, we need $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$ to imply $p > \sqrt{\frac{\tau}{3}}$.

Set $P_\tau = \{p \text{ prime } : \left(\frac{p}{\tau}\right) = 1, p \leq \sqrt{\frac{\tau}{3}}\}$.

Condition P is just: $P_\tau \subseteq K_n$

For $n = \pm 1$, $P_3 = P_5 = \emptyset$, so Condition P holds vacuously.
For $n = -4$, $P_{17} = \{2\}$; we verify condition P via $2 = 2^2 + 2(1) + (-4)(1)^2$.

Lots of computational data available.

Paying IOUs

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K_n'$.

Proof: ABWOC, $pt = a^2 + ab + nb^2$ with $\gcd(a, b) = 1$. If $p|b$, then $p|a$, contradiction. Hence pick c with $bc \equiv 1 \pmod{p}$.

Modulo p, $a^2 + ab + nb^2 \equiv b^2((ac)^2 + (ac) + n) \equiv 0 \equiv 4((ac)^2 + (ac) + n) \equiv (2ac + 1)^2 + 4n - 1$. Hence $\left(\frac{1-4n}{p}\right) = 1$. By Lemma, $\left(\frac{p}{\tau}\right) = 1$, contradiction.

Corollary: $0 \notin K_n'$ [Pays IOU in Key Lemma]
Proof: Choose p an odd quadratic nonresidue by Dirichlet's theorem, and $t = 0$.

What about $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$?

Paying IOUs

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K_n'$.

Proof: ABWOC, $pt = a^2 + ab + nb^2$ with $\gcd(a, b) = 1$. If $p|b$, then $p|a$, contradiction. Hence pick c with $bc \equiv 1 \pmod{p}$.

Modulo p, $a^2 + ab + nb^2 \equiv b^2((ac)^2 + (ac) + n) \equiv 0 \equiv 4((ac)^2 + (ac) + n) \equiv (2ac + 1)^2 + 4n - 1$. Hence $\left(\frac{1-4n}{p}\right) = 1$. By Lemma, $\left(\frac{p}{\tau}\right) = 1$, contradiction.

Corollary: $0 \notin K_n'$ [Pays IOU in Key Lemma]
Proof: Choose p an odd quadratic nonresidue by Dirichlet's theorem, and $t = 0$.

What about $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$?

Paying IOUs

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K'_n$.

Proof: ABWOC, $pt = a^2 + ab + nb^2$ with $\gcd(a, b) = 1$. If $p|b$, then $p|a$, contradiction. Hence pick c with $bc \equiv 1 \pmod{p}$.

Modulo p, $a^2 + ab + nb^2 \equiv b^2((ac)^2 + (ac) + n) \equiv 0 \equiv 4((ac)^2 + (ac) + n) \equiv (2ac + 1)^2 + 4n - 1$. Hence $\left(\frac{1-4n}{p}\right) = 1$. By Lemma, $\left(\frac{p}{\tau}\right) = 1$, contradiction.

Corollary: $0 \notin K'_n$ [Pays IOU in Key Lemma]
Proof: Choose p an odd quadratic nonresidue by Dirichlet's theorem, and $t = 0$.

What about $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$?

Paying IOUs

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K_n'$.

Proof: ABWOC, $pt = a^2 + ab + nb^2$ with $\gcd(a, b) = 1$. If $p|b$, then $p|a$, contradiction. Hence pick c with $bc \equiv 1 \pmod{p}$.

Modulo p, $a^2 + ab + nb^2 \equiv b^2((ac)^2 + (ac) + n) \equiv 0 \equiv 4((ac)^2 + (ac) + n) \equiv (2ac + 1)^2 + 4n - 1$. Hence $\left(\frac{1-4n}{p}\right) = 1$. By Lemma, $\left(\frac{p}{\tau}\right) = 1$, contradiction.

Corollary: $0 \notin K_n'$ [Pays IOU in Key Lemma]
Proof: Choose p an odd quadratic nonresidue by Dirichlet's theorem, and $t = 0$.

What about $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$?

Paying IOUs

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K'_n$.

Proof: ABWOC, $pt = a^2 + ab + nb^2$ with $\gcd(a, b) = 1$. If $p|b$, then $p|a$, contradiction. Hence pick c with $bc \equiv 1 \pmod{p}$.

Modulo p, $a^2 + ab + nb^2 \equiv b^2((ac)^2 + (ac) + n) \equiv 0 \equiv 4((ac)^2 + (ac) + n) \equiv (2ac + 1)^2 + 4n - 1$. Hence $\left(\frac{1-4n}{p}\right) = 1$. By Lemma, $\left(\frac{p}{\tau}\right) = 1$, contradiction.

Corollary: $0 \notin K'_n$ [Pays IOU in Key Lemma]
Proof: Choose p an odd quadratic nonresidue by Dirichlet's theorem, and $t = 0$.

What about $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$?

Paying IOUs, cont.

Lemma: Let $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $4t \notin K_n'$.

Proof: By QR, $|1 - 4n| = \tau \equiv \pm 3 \pmod 8$, so n odd.
ABWOC: $4t = a^2 + ab + nb^2$ with $\gcd(a, b) = 1$.

Working mod 2, we have $0 \equiv a^2 + ab + b^2 \pmod 2$. Looking at cases, must have $a \equiv b \equiv 0 \pmod 2$. But then $\gcd(a, b) \neq 1$, a contradiction.

San Diego State University

Paying IOUs, cont.

Lemma: Let $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $4t \notin K_n'$.

Proof: By QR, $|1 - 4n| = \tau \equiv \pm 3 \pmod 8$, so n odd.
ABWOC: $4t = a^2 + ab + nb^2$ with $\gcd(a, b) = 1$.

Working mod 2, we have $0 \equiv a^2 + ab + b^2 \pmod 2$. Looking at cases, must have $a \equiv b \equiv 0 \pmod 2$. But then $\gcd(a, b) \neq 1$, a contradiction.

Paying IOUs, cont.

Lemma: Let $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $4t \notin K_n'$.

Proof: By QR, $|1 - 4n| = \tau \equiv \pm 3 \pmod 8$, so n odd.
ABWOC: $4t = a^2 + ab + nb^2$ with $\gcd(a, b) = 1$.

Working mod 2, we have $0 \equiv a^2 + ab + b^2 \pmod 2$. Looking at cases, must have $a \equiv b \equiv 0 \pmod 2$. But then $\gcd(a, b) \neq 1$, a contradiction.

Paying the last IOU

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

Proof: Write $tp = a^2 + ab + nb^2$, $p = c^2 + cd + nd^2$. We calculate $b^2p - d^2tp = (bc - ad)(bd + bc + ad)$.

Case $p|(bc - ad)$: Write $rp = bc - ad$. Set $y = a + rnd$, $x = b - rc$. Plug in for a, b, cancel, rearrange to $c(x - rd) = dy$. Since $p \in K_n'$, $\gcd(c, d) = 1$, so $c|y$ and we write $y = cw$. Plug in for y, cancel, rearrange to $x = d(w + r)$. Compute $(w + wr + nr^2)(c + cd + nd^2) = \cdots = a^2 + ab + nb^2 = tp$, so $t = w^2 + wr + nr^2 \in K_n$.

Case $p|(bd + bc + ad)$: similar.

Paying the last IOU

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

Proof: Write $tp = a^2 + ab + nb^2$, $p = c^2 + cd + nd^2$. We calculate $b^2 p - d^2 tp = (bc - ad)(bd + bc + ad)$.

Case $p|(bc - ad)$: Write $rp = bc - ad$. Set $y = a + rnd$, $x = b - rc$. Plug in for a, b, cancel, rearrange to $c(x - rd) = dy$. Since $p \in K'_n$, $\gcd(c, d) = 1$, so $c|y$ and we write $y = cw$. Plug in for y, cancel, rearrange to $x = d(w + r)$. Compute $(w + wr + nr^2)(c + cd + nd^2) = \cdots = a^2 + ab + nb^2 = tp$, so $t = w^2 + wr + nr^2 \in K_n$.

Case $p|(bd + bc + ad)$: similar.

Paying the last IOU

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

Proof: Write $tp = a^2 + ab + nb^2$, $p = c^2 + cd + nd^2$. We calculate $b^2 p - d^2 tp = (bc - ad)(bd + bc + ad)$.

Case $p|(bc - ad)$: Write $rp = bc - ad$. Set $y = a + rnd$, $x = b - rc$. Plug in for a, b, cancel, rearrange to $c(x - rd) = dy$. Since $p \in K_n'$, $\gcd(c, d) = 1$, so $c|y$ and we write $y = cw$. Plug in for y, cancel, rearrange to $x = d(w + r)$. Compute $(w + wr + nr^2)(c + cd + nd^2) = \cdots = a^2 + ab + nb^2 = tp$, so $t = w^2 + wr + nr^2 \in K_n$.

Case $p|(bd + bc + ad)$: similar.

SAN DIEGO STATE UNIVERSITY

Paying the last IOU

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

Proof: Write $tp = a^2 + ab + nb^2$, $p = c^2 + cd + nd^2$. We calculate $b^2p - d^2tp = (bc - ad)(bd + bc + ad)$.

Case $p|(bc - ad)$: Write $rp = bc - ad$. Set $y = a + rnd$, $x = b - rc$. Plug in for a, b, cancel, rearrange to $c(x - rd) = dy$. Since $p \in K_n'$, $\gcd(c, d) = 1$, so $c|y$ and we write $y = cw$. Plug in for y, cancel, rearrange to $x = d(w + r)$. Compute $(w + wr + nr^2)(c + cd + nd^2) = \cdots = a^2 + ab + nb^2 = tp$, so $t = w^2 + wr + nr^2 \in K_n$.

Case $p|(bd + bc + ad)$: similar.

Remembering all the Lemmas

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K_n'$.

Lemma: Let $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $4t \notin K_n'$.

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

SAN DIEGO STATE UNIVERSITY

Main Result, Revisited

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Proof: ABWOC, p minimal prime with $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$. Condition P implies $p > \sqrt{\frac{\tau}{3}}$.

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Applying Key Lemma, choose $|t|$ minimal with $0 < |t| < p$ and $pt \in K_n'$.

$|t| = 1$ impossible. So write $|t| = p_1 p_2 \cdots p_k$, with each p_i prime and $p_i < p$.

Main Result, Revisited

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Proof: ABWOC, p minimal prime with $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$. Condition P implies $p > \sqrt{\frac{\tau}{3}}$.

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Applying Key Lemma, choose $|t|$ minimal with $0 < |t| < p$ and $pt \in K_n'$.

$|t| = 1$ impossible. So write $|t| = p_1 p_2 \cdots p_k$, with each p_i prime and $p_i < p$.

Main Result, Revisited

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Proof: ABWOC, p minimal prime with $\left(\frac{p}{\tau}\right) = 1$ and $p \notin K_n$. Condition P implies $p > \sqrt{\frac{\tau}{3}}$.

Key Lemma: Let $p \neq \tau$ be an odd, prime, quadratic residue. Then $pt \in K_n'$ for some $t \in \mathbb{Z}$. If $p > \sqrt{\frac{\tau}{3}}$, then also $0 < |t| < p$.

Applying Key Lemma, choose $|t|$ minimal with $0 < |t| < p$ and $pt \in K_n'$.

$|t| = 1$ impossible. So write $|t| = p_1 p_2 \cdots p_k$, with each p_i prime and $p_i < p$.

Main Result, Continued

$pt \in K_n'$, $|t| = p_1 p_2 \cdots p_k < p$, with each p_i prime and $p_i < p$.

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

If $p_i \in K_n$, then by Lemma $p\frac{t}{p_i} \in K_n$. Write $p\frac{t}{p_i} = a^2 + ab + nb^2$, and now $p\frac{t}{p_i \gcd(a,b)^2} \in K_n'$. Contradicts choice of t. So $p_i \notin K_n$.

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K_n'$.

If p_i is odd and $\left(\frac{p_i}{\tau}\right) = 1$, contradicts choice of p. If p_i is odd and $\left(\frac{p_i}{\tau}\right) = -1$, by lemma, $pt \notin K_n'$, a contradiction. Hence $p_i = 2$, i.e. $|t| = 2^c$ for some $c \geq 1$.

Main Result, Continued

$pt \in K_n'$, $|t| = p_1 p_2 \cdots p_k < p$, with each p_i prime and $p_i < p$.

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

If $p_i \in K_n$, then by Lemma $p\frac{t}{p_i} \in K_n$. Write $p\frac{t}{p_i} = a^2 + ab + nb^2$, and now $p\frac{t}{p_i \gcd(a,b)^2} \in K_n'$. Contradicts choice of t. So $p_i \notin K_n$.

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K_n'$.

If p_i is odd and $\left(\frac{p_i}{\tau}\right) = 1$, contradicts choice of p. If p_i is odd and $\left(\frac{p_i}{\tau}\right) = -1$, by lemma, $pt \notin K_n'$, a contradiction. Hence $p_i = 2$, i.e. $|t| = 2^c$ for some $c \geq 1$.

Main Result, Continued

$pt \in K_n'$, $|t| = p_1 p_2 \cdots p_k < p$, with each p_i prime and $p_i < p$.

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

If $p_i \in K_n$, then by Lemma $p\frac{t}{p_i} \in K_n$. Write $p\frac{t}{p_i} = a^2 + ab + nb^2$, and now $p\frac{t}{p_i \gcd(a,b)^2} \in K_n'$. Contradicts choice of t. So $p_i \notin K_n$.

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K_n'$.

If p_i is odd and $\left(\frac{p_i}{\tau}\right) = 1$, contradicts choice of p. If p_i is odd and $\left(\frac{p_i}{\tau}\right) = -1$, by lemma, $pt \notin K_n'$, a contradiction. Hence $p_i = 2$, i.e. $|t| = 2^c$ for some $c \geq 1$.

San Diego State University

Main Result, Continued

$pt \in K_n'$, $|t| = p_1 p_2 \cdots p_k < p$, with each p_i prime and $p_i < p$.

Lemma: Let $p, t \in \mathbb{N}$ with p prime. If $tp, p \in K_n$, then $t \in K_n$.

If $p_i \in K_n$, then by Lemma $p\frac{t}{p_i} \in K_n$. Write $p\frac{t}{p_i} = a^2 + ab + nb^2$, and now $p\frac{t}{p_i \gcd(a,b)^2} \in K_n'$. Contradicts choice of t. So $p_i \notin K_n$.

Lemma: Let $p \neq \tau$ be odd prime with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $pt \notin K_n'$.

If p_i is odd and $\left(\frac{p_i}{\tau}\right) = 1$, contradicts choice of p. If p_i is odd and $\left(\frac{p_i}{\tau}\right) = -1$, by lemma, $pt \notin K_n'$, a contradiction. Hence $p_i = 2$, i.e. $|t| = 2^c$ for some $c \geq 1$.

Main Result, Concluded

$pt \in K_n'$, $\left(\frac{2}{\tau}\right) = -1$, $|t| = 2^c$ for some $c \geq 1$.

Lemma: Let $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $4t \notin K_n'$.

If $c \geq 2$, apply Lemma to get $pt \notin K_n'$, a contradiction. Hence $c = 1$, i.e. $|t| = 2$.

Finally, we are left with $2p \in K_n'$, $\left(\frac{2}{\tau}\right) = -1$. But then $\left(\frac{2p}{\tau}\right) = \left(\frac{2}{\tau}\right)\left(\frac{p}{\tau}\right) = -1$, a contradiction. $\square$

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Main Result, Concluded

$pt \in K_n'$, $\left(\frac{2}{\tau}\right) = -1$, $|t| = 2^c$ for some $c \geq 1$.

Lemma: Let $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $4t \notin K_n'$.

If $c \geq 2$, apply Lemma to get $pt \notin K_n'$, a contradiction. Hence $c = 1$, i.e. $|t| = 2$.

Finally, we are left with $2p \in K_n'$, $\left(\frac{2}{\tau}\right) = -1$. But then $\left(\frac{2p}{\tau}\right) = \left(\frac{2}{\tau}\right)\left(\frac{p}{\tau}\right) = -1$, a contradiction. $\square$

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Main Result, Concluded

$pt \in K'_n$, $\left(\frac{2}{\tau}\right) = -1$, $|t| = 2^c$ for some $c \geq 1$.

Lemma: Let $p = 2$ with $\left(\frac{p}{\tau}\right) = -1$, and $t \in \mathbb{Z}$. Then $4t \notin K'_n$.

If $c \geq 2$, apply Lemma to get $pt \notin K'_n$, a contradiction. Hence $c = 1$, i.e. $|t| = 2$.

Finally, we are left with $2p \in K'_n$, $\left(\frac{2}{\tau}\right) = -1$. But then $\left(\frac{2p}{\tau}\right) = \left(\frac{2}{\tau}\right)\left(\frac{p}{\tau}\right) = -1$, a contradiction. $\square$

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Monoids...?

Lemma: $\tau \in K_n$.

Lemma: If $t \neq \tau$ is a quadratic nonresidue mod τ, then $t \notin K_n$.

Lemma: For any $x \in \mathbb{N}$, $x^2 \in K_n$.

Thm: Assume Condition P. If p prime with $\left(\frac{p}{\tau}\right) = 1$, then $p \in K_n$.

Monoid irreducibles: τ, residues p, nonresidues q^2, others?

No others

Theorem: Assume Condition P. The irreducibles in $K_n \cap \mathbb{N}$ are: τ, p (for prime residues p), q^2 (for prime nonresidues q).

Proof: Suppose $t = p_1 p_2 \cdots p_k$ is irreducible in K_n, of no other type. Note $k \geq 2$. If any $p_i \in K_n$, then $\frac{t}{p_i} \in K_n$ by Lemma, contradicting irreducible. If any p_i is odd, then by Lemma $t \notin K_n'$. Since $t \in K_n$, we have $t = a^2 + ab + nb^2$ with $r = \gcd(a, b) > 1$. But then $r^2, \frac{t}{r^2} \in K_n$, contradicting irreducible. Hence each $p_i = 2$. If k is even, contradicts irreducible. If k is odd, t is nonresidue.

No others

Theorem: Assume Condition P. The irreducibles in $K_n \cap \mathbb{N}$ are: τ, p (for prime residues p), q^2 (for prime nonresidues q).

Proof: Suppose $t = p_1 p_2 \cdots p_k$ is irreducible in K_n, of no other type. Note $k \geq 2$. If any $p_i \in K_n$, then $\frac{t}{p_i} \in K_n$ by Lemma, contradicting irreducible. If any p_i is odd, then by Lemma $t \notin K_n'$. Since $t \in K_n$, we have $t = a^2 + ab + nb^2$ with $r = \gcd(a, b) > 1$. But then $r^2, \frac{t}{r^2} \in K_n$, contradicting irreducible. Hence each $p_i = 2$. If k is even, contradicts irreducible. If k is odd, t is nonresidue.

No others

Theorem: Assume Condition P. The irreducibles in $K_n \cap \mathbb{N}$ are: τ, p (for prime residues p), q^2 (for prime nonresidues q).

Proof: Suppose $t = p_1 p_2 \cdots p_k$ is irreducible in K_n, of no other type. Note $k \geq 2$. If any $p_i \in K_n$, then $\frac{t}{p_i} \in K_n$ by Lemma, contradicting irreducible. If any p_i is odd, then by Lemma $t \notin K_n'$. Since $t \in K_n$, we have $t = a^2 + ab + nb^2$ with $r = \gcd(a, b) > 1$. But then $r^2, \frac{t}{r^2} \in K_n$, contradicting irreducible. Hence each $p_i = 2$. If k is even, contradicts irreducible. If k is odd, t is nonresidue.

Representation Characterization

Theorem: Consider form $x^2 + xy + ny^2$, with $\tau = |1 - 4n|$ prime. Assume Condition P. Natural t is represented by $x^2 + xy + ny^2$, iff every prime dividing t that is a quadratic nonresidue modulo τ, appears to an even power.

Generalizing

Given a principal binary quadratic form $x^2 + mxy + ny^2$,

If $\tau = |m^2 - 4n|$ is prime, then m is odd, and

using substitution $\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & (1-m)/2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

turns the form into $x^2 + xy + \frac{1-m^2+4n}{4} y^2$.

Note: $\tau = |m^2 - 4n|$ unchanged, monoid unchanged
"Properly equivalent"

Generalizing

Given a principal binary quadratic form $x^2 + mxy + ny^2$,

If $\tau = |m^2 - 4n|$ is prime, then m is odd, and

using substitution $\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} 1 & (1-m)/2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

turns the form into $x^2 + xy + \frac{1-m^2+4n}{4} y^2$.

Note: $\tau = |m^2 - 4n|$ unchanged, monoid unchanged

"Properly equivalent"

Generalizing

Given a principal binary quadratic form $x^2 + mxy + ny^2$,

If $\tau = |m^2 - 4n|$ is prime, then m is odd, and

using substitution $\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} 1 & (1-m)/2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

turns the form into $x^2 + xy + \frac{1-m^2+4n}{4} y^2$.

Note: $\tau = |m^2 - 4n|$ unchanged, monoid unchanged
"Properly equivalent"

Various Equivalences

proper equivalence: $\begin{bmatrix} x \\ y \end{bmatrix} \to A \begin{bmatrix} x \\ y \end{bmatrix}$ with $A \in SL_n(\mathbb{Z})$, i.e. $|A| = 1$

wide equivalence: $\begin{bmatrix} x \\ y \end{bmatrix} \to A \begin{bmatrix} x \\ y \end{bmatrix}$ with $A \in GL_n(\mathbb{Z})$, i.e. $|A| = \pm 1$

image equivalence: The forms share the same image in $\mathbb{Z}$

(proper equiv.)$\to$(wide equiv.)$\to$(image equiv.)
All preserve discriminant.

Various Equivalences

proper equivalence: $\begin{bmatrix} x \\ y \end{bmatrix} \to A \begin{bmatrix} x \\ y \end{bmatrix}$ with $A \in SL_n(\mathbb{Z})$, i.e. $|A| = 1$

wide equivalence: $\begin{bmatrix} x \\ y \end{bmatrix} \to A \begin{bmatrix} x \\ y \end{bmatrix}$ with $A \in GL_n(\mathbb{Z})$, i.e. $|A| = \pm 1$

image equivalence: The forms share the same image in $\mathbb{Z}$

(proper equiv.)$\to$(wide equiv.)$\to$(image equiv.)
All preserve discriminant.

Various Equivalences

proper equivalence: $\begin{bmatrix} x \\ y \end{bmatrix} \to A \begin{bmatrix} x \\ y \end{bmatrix}$ with $A \in SL_n(\mathbb{Z})$, i.e. $|A| = 1$

wide equivalence: $\begin{bmatrix} x \\ y \end{bmatrix} \to A \begin{bmatrix} x \\ y \end{bmatrix}$ with $A \in GL_n(\mathbb{Z})$, i.e. $|A| = \pm 1$

image equivalence: The forms share the same image in $\mathbb{Z}$

(proper equiv.)$\to$(wide equiv.)$\to$(image equiv.)
All preserve discriminant.

Various Equivalences

proper equivalence: $\begin{bmatrix} x \\ y \end{bmatrix} \to A \begin{bmatrix} x \\ y \end{bmatrix}$ with $A \in SL_n(\mathbb{Z})$, i.e. $|A| = 1$

wide equivalence: $\begin{bmatrix} x \\ y \end{bmatrix} \to A \begin{bmatrix} x \\ y \end{bmatrix}$ with $A \in GL_n(\mathbb{Z})$, i.e. $|A| = \pm 1$

image equivalence: The forms share the same image in $\mathbb{Z}$

(proper equiv.)$\to$(wide equiv.)$\to$(image equiv.)
All preserve discriminant.

Quadratic Forms

My naive approach: Given form, find its image.

Traditional approach: Given integer in image, find form that represents it.

For discriminant Δ:
$\Delta < 0$: "positive definite", $h(D) = \#$ proper equivalence classes
$\Delta > 0$: "indefinite", $h^+(D) = \#$ proper equivalence classes

"class numbers"

Quadratic Forms

My naive approach: Given form, find its image.

Traditional approach: Given integer in image, find form that represents it.

For discriminant Δ:
$\Delta < 0$: "positive definite", $h(D) = \#$ proper equivalence classes
$\Delta > 0$: "indefinite", $h^{+}(D) = \#$ proper equivalence classes

"class numbers"

Quadratic Forms

My naive approach: Given form, find its image.

Traditional approach: Given integer in image, find form that represents it.

For discriminant Δ:
$\Delta < 0$: "positive definite", $h(D) = \#$ proper equivalence classes
$\Delta > 0$: "indefinite", $h^{+}(D) = \#$ proper equivalence classes

"class numbers"

Quadratic Forms

My naive approach: Given form, find its image.

Traditional approach: Given integer in image, find form that represents it.

For discriminant Δ:
$\Delta < 0$: "positive definite", $h(D) = \#$ proper equivalence classes
$\Delta > 0$: "indefinite", $h^{+}(D) = \#$ proper equivalence classes

"class numbers"

Positive Definite Forms

Lemma: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. If prime $p \in K_n$, then $p \geq \frac{\tau}{4}$.
Proof: Suppose $x^2 + xy + ny^2 = p$. Quadratic formula gives $x = \frac{1}{2}(-y \pm \sqrt{-\tau y^2 + 4p})$, so $-\tau y^2 + 4p \geq 0$. $y = 0$ impossible, so $y^2 \geq 1$. Hence $p \geq \frac{\tau}{4}$.

Theorem: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff $P_\tau = \emptyset$.

Proof: $P_\tau = \{p \text{ prime } : \left(\frac{p}{\tau}\right) = 1, p \leq \sqrt{\frac{\tau}{3}}\} \overset{?}{\subseteq} K_n$. $\quad \frac{\tau}{4} \leq p \leq \sqrt{\frac{\tau}{3}}$

Corollary: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff the least prime quadratic residue modulo τ is $> \sqrt{\frac{\tau}{3}}$.

Positive Definite Forms

Lemma: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. If prime $p \in K_n$, then $p \geq \frac{\tau}{4}$.
Proof: Suppose $x^2 + xy + ny^2 = p$. Quadratic formula gives $x = \frac{1}{2}(-y \pm \sqrt{-\tau y^2 + 4p})$, so $-\tau y^2 + 4p \geq 0$. $y = 0$ impossible, so $y^2 \geq 1$. Hence $p \geq \frac{\tau}{4}$.

Theorem: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff $P_\tau = \emptyset$.

Proof: $P_\tau = \{p \text{ prime } : \left(\frac{p}{\tau}\right) = 1, p \leq \sqrt{\frac{\tau}{3}}\} \overset{?}{\subseteq} K_n$. $\quad \frac{\tau}{4} \leq p \leq \sqrt{\frac{\tau}{3}}$

Corollary: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff the least prime quadratic residue modulo τ is $> \sqrt{\frac{\tau}{3}}$.

Positive Definite Forms

Lemma: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. If prime $p \in K_n$, then $p \geq \frac{\tau}{4}$.
Proof: Suppose $x^2 + xy + ny^2 = p$. Quadratic formula gives $x = \frac{1}{2}(-y \pm \sqrt{-\tau y^2 + 4p})$, so $-\tau y^2 + 4p \geq 0$. $y = 0$ impossible, so $y^2 \geq 1$. Hence $p \geq \frac{\tau}{4}$.

Theorem: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff $P_\tau = \emptyset$.

Proof: $P_\tau = \{p \text{ prime } : \left(\frac{p}{\tau}\right) = 1, p \leq \sqrt{\frac{\tau}{3}}\} \overset{?}{\subseteq} K_n$. $\quad \frac{\tau}{4} \leq p \leq \sqrt{\frac{\tau}{3}}$

Corollary: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff the least prime quadratic residue modulo τ is $> \sqrt{\frac{\tau}{3}}$.

Positive Definite Forms

Lemma: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. If prime $p \in K_n$, then $p \geq \frac{\tau}{4}$.
Proof: Suppose $x^2 + xy + ny^2 = p$. Quadratic formula gives $x = \frac{1}{2}(-y \pm \sqrt{-\tau y^2 + 4p})$, so $-\tau y^2 + 4p \geq 0$. $y = 0$ impossible, so $y^2 \geq 1$. Hence $p \geq \frac{\tau}{4}$.

Theorem: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff $P_\tau = \emptyset$.

Proof: $P_\tau = \{p \text{ prime } : \left(\frac{p}{\tau}\right) = 1, p \leq \sqrt{\frac{\tau}{3}}\} \overset{?}{\subseteq} K_n$. $\quad \frac{\tau}{4} \leq p \leq \sqrt{\frac{\tau}{3}}$

Corollary: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff the least prime quadratic residue modulo τ is $> \sqrt{\frac{\tau}{3}}$.

SAN DIEGO STATE UNIVERSITY

Positive Definite Forms, cont.

Corollary: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff the least quadratic residue modulo τ is $> \sqrt{\frac{\tau}{3}}$.

Theorem [Chowla Cowles Cowles 1986]: Let $\tau > 3$ be prime with $\tau \equiv 3 \pmod 8$. Then the least prime quadratic residue modulo τ is:

$$\begin{cases} < \sqrt{\frac{\tau}{3}} & h(-\tau) > 1 \\ = \frac{\tau+1}{4} & h(-\tau) = 1. \end{cases}$$

For $n > 0$, we have (Class number 1) $\leftrightarrow$ (Condition P)

Positive Definite Forms, cont.

Corollary: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff the least quadratic residue modulo τ is $> \sqrt{\frac{\tau}{3}}$.

Theorem [Chowla Cowles Cowles 1986]: Let $\tau > 3$ be prime with $\tau \equiv 3 \pmod 8$. Then the least prime quadratic residue modulo τ is:

$$\begin{cases} < \sqrt{\frac{\tau}{3}} & h(-\tau) > 1 \\ = \frac{\tau+1}{4} & h(-\tau) = 1. \end{cases}$$

For $n > 0$, we have (Class number 1) $\leftrightarrow$ (Condition P)

Positive Definite Forms, cont.

Corollary: Consider $x^2 + xy + ny^2$, with $n > 0$ and $\tau = 4n - 1$ prime. Then Condition P holds iff the least quadratic residue modulo τ is $> \sqrt{\frac{\tau}{3}}$.

Theorem [Chowla Cowles Cowles 1986]: Let $\tau > 3$ be prime with $\tau \equiv 3 \pmod 8$. Then the least prime quadratic residue modulo τ is:

$$\begin{cases} < \sqrt{\frac{\tau}{3}} & h(-\tau) > 1 \\ = \frac{\tau+1}{4} & h(-\tau) = 1. \end{cases}$$

For $n > 0$, we have (Class number 1) $\leftrightarrow$ (Condition P)

Positive Definite Forms Wrapup

For $n > 0$, we have (Class number 1) $\leftrightarrow$ (Condition P)

Theorem [Baker-Heegner-Stark]:
For $\Delta < 0$, the (narrow) class number of $\mathbb{Q}[\sqrt{\Delta}] = 1$, iff $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$

Corollary: For $n > 0$ and τ prime, Condition P holds iff $\tau \in \{3, 7, 11, 19, 43, 67, 163\}$

SAN DIEGO STATE UNIVERSITY

Positive Definite Forms Wrapup

For $n > 0$, we have (Class number 1) $\leftrightarrow$ (Condition P)

Theorem [Baker-Heegner-Stark]:
For $\Delta < 0$, the (narrow) class number of $\mathbb{Q}[\sqrt{\Delta}] = 1$, iff $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$

Corollary: For $n > 0$ and τ prime, Condition P holds iff $\tau \in \{3, 7, 11, 19, 43, 67, 163\}$

Indefinite Forms

For $n < 0$, we have (Class number 1) $\rightarrow$ (Condition P)

If τ is prime with $\tau \equiv 1 \pmod 4$, and $\mathbb{Q}[\sqrt{\tau}]$ has narrow class number 1, then Condition P holds.

Condition P holds for $\tau \in \{5, 13, 17, 29, 37, 41, 53, \ldots\}$.

Open problem: Are there infinitely many $\tau \equiv 1 \pmod 4$ with $\mathbb{Q}[\sqrt{\tau}]$ having narrow class number 1?

Indefinite Forms

For $n < 0$, we have (Class number 1) $\rightarrow$ (Condition P)

If τ is prime with $\tau \equiv 1 \pmod 4$, and $\mathbb{Q}[\sqrt{\tau}]$ has narrow class number 1, then Condition P holds.

Condition P holds for $\tau \in \{5, 13, 17, 29, 37, 41, 53, \ldots\}$.

Open problem: Are there infinitely many $\tau \equiv 1 \pmod 4$ with $\mathbb{Q}[\sqrt{\tau}]$ having narrow class number 1?

Indefinite Forms

For $n < 0$, we have (Class number 1) $\rightarrow$ (Condition P)

If τ is prime with $\tau \equiv 1 \pmod 4$, and $\mathbb{Q}[\sqrt{\tau}]$ has narrow class number 1, then Condition P holds.

Condition P holds for $\tau \in \{5, 13, 17, 29, 37, 41, 53, \ldots\}$.

Open problem: Are there infinitely many $\tau \equiv 1 \pmod 4$ with $\mathbb{Q}[\sqrt{\tau}]$ having narrow class number 1?

What Happens Next. . . ?

1. Paper with Dimabayao and Tigas
2. For $n < 0$, do we have (Class number 1) $\leftrightarrow$ (Condition P)? (genera?)
3. For $n > 0$, can we disprove Condition P directly? Elementary proof of Baker-Heegner-Stark
4. If Condition P fails, what can we salvage? Monoid?
5. $\tau = 23$ minimal with $n > 0$; $\tau = 229$ minimal with $n < 0$.
6. Non-principal forms, non-prime τ. . .

What Happens Next...?

1. Paper with Dimabayao and Tigas
2. For $n < 0$, do we have (Class number 1) $\leftrightarrow$ (Condition P)? (genera?)
3. For $n > 0$, can we disprove Condition P directly? Elementary proof of Baker-Heegner-Stark
4. If Condition P fails, what can we salvage? Monoid?
5. $\tau = 23$ minimal with $n > 0$; $\tau = 229$ minimal with $n < 0$.
6. Non-principal forms, non-prime τ...

San Diego State University

What Happens Next. . . ?

1. Paper with Dimabayao and Tigas
2. For $n < 0$, do we have (Class number 1) $\leftrightarrow$ (Condition P)? (genera?)
3. For $n > 0$, can we disprove Condition P directly? Elementary proof of Baker-Heegner-Stark
4. If Condition P fails, what can we salvage? Monoid?
5. $\tau = 23$ minimal with $n > 0$; $\tau = 229$ minimal with $n < 0$.
6. Non-principal forms, non-prime τ. . .

What Happens Next. . . ?

1. Paper with Dimabayao and Tigas
2. For $n < 0$, do we have (Class number 1) $\leftrightarrow$ (Condition P)? (genera?)
3. For $n > 0$, can we disprove Condition P directly? Elementary proof of Baker-Heegner-Stark
4. If Condition P fails, what can we salvage? Monoid?
5. $\tau = 23$ minimal with $n > 0$; $\tau = 229$ minimal with $n < 0$.
6. Non-principal forms, non-prime τ. . .

What Happens Next. . . ?

1. Paper with Dimabayao and Tigas
2. For $n < 0$, do we have (Class number 1) $\leftrightarrow$ (Condition P)? (genera?)
3. For $n > 0$, can we disprove Condition P directly? Elementary proof of Baker-Heegner-Stark
4. If Condition P fails, what can we salvage? Monoid?
5. $\tau = 23$ minimal with $n > 0$; $\tau = 229$ minimal with $n < 0$.
6. Non-principal forms, non-prime τ. . .

What Happens Next...?

1. Paper with Dimabayao and Tigas
2. For $n < 0$, do we have (Class number 1) $\leftrightarrow$ (Condition P)? (genera?)
3. For $n > 0$, can we disprove Condition P directly? Elementary proof of Baker-Heegner-Stark
4. If Condition P fails, what can we salvage? Monoid?
5. $\tau = 23$ minimal with $n > 0$; $\tau = 229$ minimal with $n < 0$.
6. Non-principal forms, non-prime τ...

For Further Reading

- S. Chowla, J. Cowles, M. Cowles
  The Least Prime Quadratic Residue and the Class Number
  J. Number Theory 22 (1986), pp. 1-3.
- K. Bahmanpour
  Prime numbers p with expression $p = a^2 \pm ab \pm b^2$
  J. Number Theory 166 (2016), pp. 208-218.
- J.T. Dimabayao, VP, O.J.Q. Tigas
  On Monic Binary Quadratic Forms
  https://vadim.sdsu.edu/qf.pdf

San Diego State University