Basics of binary quadratic forms and Gauss composition

Andrew Granville
Université de Montréal

SMS summer school: “Counting arithmetic objects”
Monday June 23rd, 2014, 3:30-5:00 pm
Any prime \( p \equiv 1 \pmod{4} \) can be written as the sum of two squares

“Geometry of numbers type” proof

Since \( p \equiv 1 \pmod{4} \implies \exists i \in \mathbb{Z} : i^2 \equiv -1 \pmod{p} \).

Idea: Find smallest non-zero integer lattice point

\((x, y) \in \mathbb{Z}^2 : x \equiv iy \pmod{p}\)
Since $p \equiv 1 \pmod{4}$ $\implies \exists i \in \mathbb{Z} : i^2 \equiv -1 \pmod{p}$.

Consider now the set of integers

$$\{m + ni : 0 \leq m, n \leq \lceil \sqrt{p} \rceil\}$$

# pairs $m, n$ is $(\lceil \sqrt{p} \rceil + 1)^2 > p$, so by the pigeonhole principle, two are congruent mod $p$; say that

$$m + ni \equiv M + Ni \pmod{p}$$

where $0 \leq m, n, M, N \leq \lceil \sqrt{p} \rceil$ and $(m, n) \neq (M, n)$.

Let $r = m - M$ and $s = N - n$ so that

$$r \equiv is \pmod{p}$$

where $|r|, |s| \leq \lceil \sqrt{p} \rceil < \sqrt{p}$, and $r$ and $s$ are not both 0.

Now

$$r^2 + s^2 \equiv (is)^2 + s^2 = s^2(i^2 + 1) \equiv 0 \pmod{p}$$

and $0 < r^2 + s^2 < \sqrt{p^2 + \sqrt{p^2}} = 2p$. The only multiple of $p$ between 0 and $2p$ is $p$, and therefore $r^2 + s^2 = p$. 
What integers can be written as the sum of two squares?

\[(a^2 + b^2)(c^2 + e^2) = (ac + be)^2 + (ae - bc)^2.\]

Generalization:
\[(a^2 + db^2)(c^2 + de^2) = (ac + dbe)^2 + d(ae - bc)^2.\]

Gauss’s view:
A binary quadratic form is of the shape
\[f(x, y) := ax^2 + bxy + cy^2.\]
Here we take \(f(x, y) = x^2 + dy^2\) and
\[f(a, b)f(c, e) = f(ac + dbe, ae - bc)\]
The latter values in \(f\), namely \(ac + dbe\) and \(ae - bc\), are bilinear forms in \(a, b, c, e\).
Does this generalize to other such multiplications?
Pell’s equation

Are there integer solutions $x, y$ to

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

Can always be found using continued fraction for $\sqrt{d}$. (Brahmagupta, 628 A.D.; probably Archimedes, to solve his “Cattle Problem” one needs to find a solution to

$$u^2 - 609 \cdot 7766v^2 = 1.$$ 

The smallest solution has about $2 \cdot 10^6$ digits!)

**Solution to Pell’s Equation**  
Let $d \geq 2$ be a non-square integer.  

$\exists x, y \in \mathbb{Z}$ for which

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

with $y \neq 0$. If $x_1, y_1$ \textit{smallest positive solution}, then all others given by

$$x_n + \sqrt{d}y_n = (x + \sqrt{d}y)^n$$
\[ x^2 - dy^2 = 1? \]

**Solution to Pell’s Equation**  
Let \( d \geq 2 \) be a non-square integer. \( \exists x, y \in \mathbb{Z} \) for which \[ x^2 - dy^2 = 1, \]
with \( y \neq 0 \). If \( x_1, y_1 \) smallest positive solution, then all others given by \[ x_n + \sqrt{d}y_n = (x + \sqrt{d}y)^n. \]

Better to look for solutions to \[ x^2 - dy^2 = \pm 4, \]
Understanding when there is solution with “−” is a difficult question (great recent progress by Fouvry and Kluners).
Theorem Any quadratic irrational real number has a continued fraction that is eventually periodic.

Here are some examples of the continued fraction for $\sqrt{d}$:

\[
\sqrt{2} = [1, \overline{2}], \quad \sqrt{3} = [1, \overline{1, 2}], \quad \sqrt{5} = [2, \overline{4}],
\]
\[
\sqrt{6} = [2, \overline{2, 4}],
\]
\[
\sqrt{7} = [2, \overline{1, 1, 1, 4}],
\]
\[
\sqrt{8} = [2, \overline{1, 4}],
\]
\[
\sqrt{10} = [3, \overline{6}],
\]
\[
\sqrt{11} = [3, \overline{3, 6}],
\]
\[
\sqrt{12} = [3, \overline{2, 6}],
\]
\[
\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}], \ldots
\]

If $p_k/q_k$ are the convergents for $\sqrt{d}$ then
\[
p_{n-1}^2 - dq_{n-1}^2 = (-1)^n.
\]
Longest continued fractions and the largest fundamental solutions

\[
\sqrt{2} = [1, 2], \quad 1^2 - 2 \cdot 1^2 = -1
\]
\[
\sqrt{3} = [1, 1, 2], \quad 2^2 - 3 \cdot 1^2 = 1
\]
\[
\sqrt{6} = [2, 2, 4], \quad 5^2 - 6 \cdot 2^2 = 1
\]
\[
\sqrt{7} = [2, 1, 1, 1, 4], \quad 8^2 - 7 \cdot 3^2 = 1
\]
\[
\sqrt{13} = [3, 1, 1, 1, 6], \quad 18^2 - 13 \cdot 5^2 = -1
\]
\[
\sqrt{19} = [4, 2, 1, 3, 1, 2, 8], \quad 170^2 - 19 \cdot 39^2 = 1
\]
\[
\sqrt{22} = [4, 1, 2, 4, 2, 1, 8], \quad 197^2 - 22 \cdot 42^2 = 1
\]
\[
\sqrt{31} = [5, 1, 1, 3, 5, 3, 1, 1, 10], \quad 1520^2 - 31 \cdot 273^2 = 1
\]
\[
\sqrt{43} = [6, 1, 1, 3, 1, 5, 1, 3, 1, 1, 12], \quad 3482^2 - 43 \cdot 531^2 = 1
\]
\[
\sqrt{46} = [6, 1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 1, 12], \quad 24335^2 - 46 \cdot 3588^2 = 1
\]
\[
\sqrt{76} = [8, 1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16], \quad 57799^2 - 76 \cdot 6630^2 = 1
\]
Length of longest cont fracts and fundl solutions

16 : \(2143295^2 - 94 \cdot 221064^2 = 1\)
16 : \(4620799^2 - 124 \cdot 414960^2 = 1\)
16 : \(2588599^2 - 133 \cdot 224460^2 = 1\)
18 : \(77563250^2 - 139 \cdot 6578829^2 = 1\)
20 : \(1728148040^2 - 151 \cdot 140634693^2 = 1\)
22 : \(1700902565^2 - 166 \cdot 132015642^2 = 1\)
26 : \(278354373650^2 - 211 \cdot 19162705353^2 = 1\)
26 : \(695359189925^2 - 214 \cdot 47533775646^2 = 1\)
26 : \(5883392537695^2 - 301 \cdot 339113108232^2 = 1\)
34 : \(2785589801443970^2 - 331 \cdot 153109862634573^2 = 1\)
37 : \(44042445696821418^2 - 421 \cdot 2146497463530785^2 = -1\)
40 : \(84056091546952933775^2 - 526 \cdot 3665019757324295532^2 = 1\)
42 : \(181124355061630786130^2 - 571 \cdot 7579818350628982587^2 = 1\)
Length of fundamental solutions

The length of the continued fractions here are around $2\sqrt{d}$, and the size of the fundamental solutions $10\sqrt{d}$.

*How big is the smallest solution?*

We believe that the smallest solution is typically of size $C\sqrt{d}$ but not much proved.

*Understanding the distribution of sizes of the smallest solutions to Pell’s equation is an outstanding open question in number theory.*
Descent on solutions of $x^2 - dy^2 = n$, $d > 0$

Let $\epsilon_d = x_1 + y_1 \sqrt{d}$, the smallest solution $x_1, y_1$ in positive integers to

$$x_1^2 - dy_1^2 = 1.$$ 

Given a solution of

$$x^2 - dy^2 = n$$

with $x, y \geq 0$, let

$$\alpha := x + y \sqrt{d} > \sqrt{n}.$$ 

If $\sqrt{n} \epsilon_d^k \leq \alpha < \sqrt{n} \epsilon_d^{k+1}$ let

$$\beta := \alpha \epsilon_d^{-k} = u + \sqrt{dv}$$

so that

$$\sqrt{n} \leq \beta < \sqrt{n} \epsilon_d$$

with $u, v \geq 1$ and $u^2 - dv^2 = n$. 
Representation of integers by binary quadratic forms

What integers are represented by *binary quadratic form* \( f(x, y) := ax^2 + bxy + cy^2 \)?

That is, for what \( N \) are there coprime \( m, n \) such that

\[ N = am^2 + bmn + cn^2 \]

WLOG \( \gcd(a, b, c) = 1 \). Complete the square to obtain

\[ 4aN = (2am + bn)^2 - dn^2 \]

where *discriminant* \( d := b^2 - 4ac \), so

\[ d \equiv 0 \text{ or } 1 \pmod{4}. \]

When \( d < 0 \) the right side can only take positive values ...
... easier than when \( d > 0 \).

If \( a > 0 \) then *positive definite* binary quadratic form.
$x^2 + y^2$ represents the same integers as $X^2 + 2XY + 2Y^2$

If $N = m^2 + n^2$ then $N = (m - n)^2 + 2(m - n)n + 2n^2$,

If $N = u^2 + 2uv + 2v^2$ then $N = (u + v)^2 + v^2$.

$$\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} X \\ Y \end{pmatrix}$$ where $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

transforms $x^2 + y^2$ into $X^2 + 2XY + 2Y^2$, and the transformation is invertible, since $\det M = 1$.

Much more generally define

$$\text{SL}(2, \mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{Z} \text{ and } \alpha \delta - \beta \gamma = 1 \right\}.$$ 

Then $ax^2 + bxy + cy^2$ represents the same integers as $AX^2 + BXY + CY^2$ whenever $$\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} X \\ Y \end{pmatrix}$$ with $M \in \text{SL}(2, \mathbb{Z})$. These quadratic forms are equivalent.
Equivalence

\( ax^2 + bxy + cy^2 \) is equivalent to \( AX^2 + BXY + CY^2 \)
if equal whenever \( \begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} X \\ Y \end{pmatrix} \) with \( M \in \text{SL}(2, \mathbb{Z}) \).

This yields an equivalence relation and splits the binary quadratic forms into equivalence classes. Write

\[
ax^2 + bxy + cy^2 = (x \ y) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} (x \ y)
\]

Discriminant(\( f \)) = \(-\det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\). We deduce that

\[
AX^2 + BXY + CY^2 = (X \ Y) M^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M \begin{pmatrix} X \\ Y \end{pmatrix},
\]

so \( A = a\alpha^2 + b\alpha\gamma + c\gamma^2 \) and \( C = a\beta^2 + b\beta\delta + c\delta^2 \) as

\[
\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} = M^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M.
\]

Hence two equivalent bqfs have same discriminant.
Equivalence classes of binary quadratic forms

$29X^2 + 82XY + 58Y^2$ is equivalent to $x^2 + y^2$

Gauss: Every equivalence class of bqfs (with $d < 0$) contains a unique reduced representative, defined as

$-a < b \leq a \leq c$, and $b \geq 0$ whenever $a = c$.

If so, $|d| = 4ac - (|b|)^2 \geq 4a \cdot a - a^2 = 3a^2$ and hence

$$a \leq \sqrt{|d|/3}.$$  

Therefore, for given $d < 0$, finitely many $a$, and so $b$ (as $|b| \leq a$), and then $c = (b^2 - d)/4a$ is determined; so only finitely many ($h(d)$, the class number, the number of equivalence classes) reduced bqfs of discrim $d$. In fact $h(d) \geq 1$ since we always have the principal form:

$$\begin{cases} 
  x^2 - (d/4)y^2 & \text{when } d \equiv 0 \pmod{4}, \\
  x^2 + xy + (1-d)/4y^2 & \text{when } d \equiv 1 \pmod{4}.
\end{cases}$$
Gauss’s reduction Theorem

Every positive definite binary quadratic form is properly equivalent to a reduced form.

i) If $c < a$ the transformation \[
\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix},
\]
yields $(c, -b, a)$ which is properly equivalent to $(a, b, c)$.

ii) If $b > a$ or $b \leq -a$ let $b'$ be the least residue, in absolute value, of $b \pmod{2a}$, so $-a < b' \leq a$, say $b' = b - 2ka$. Then let \[
\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 - k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.
\]
The resulting form $(a, b', c')$ is properly equivalent to $(a, b, c)$.

iii) If $c = a$ and $-a < b < 0$ then we use the transformation \[
\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}
\]
yielding the form $(a, -b, a)$.

If resulting form not reduced, \textbf{repeat}
Gauss’s reduction Theorem

Every positive definite binary quadratic form is properly equivalent to a reduced form.

i) If \( c < a \) then \[
\begin{pmatrix}
  x \\
  y
\end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix}
  x' \\
  y'
\end{pmatrix}.
\]

ii) If \( b > a \) or \( b \leq -a \) then \[
\begin{pmatrix}
  x \\
  y
\end{pmatrix} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix}
  x' \\
  y'
\end{pmatrix}.
\]

iii) If \( c = a \) and \( -a < b < 0 \) then \[
\begin{pmatrix}
  x \\
  y
\end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix}
  x' \\
  y'
\end{pmatrix}
\]

If resulting form not reduced, repeat

The algorithm terminates after (iii), and since (ii) is followed by (i) or (iii), and since (i) reduces the size of \( a \).
Gauss’s reduction Theorem; examples

(76, 217, 155) of discriminant $-31$, The sequence of forms is

(76, 65, 14), (14, $-65$, 76), (14, $-9$, 2), (2, 9, 14), (2, 1, 4),

the sought after reduced form.

(11, 49, 55) of discriminant $-19$, gives the sequence of forms

(11, 5, 1), (1, $-5$, 11), (1, 1, 5).
Restriction on values taken by a bqf

Suppose $d = b^2 - 4ac$ with $(a, b, c) = 1$, and $p$ is a prime.

- (i) If $p = am^2 + bmn + cn^2$ for some integers $m, n$ then $d$ is a square mod $4p$.

- (ii) If $d$ is a square mod $4p$ then there exists a binary quadratic form of discriminant $d$ that represents $p$.

Proof. (i) If $p \nmid 2ad$ and $p = am^2 + bmn + cn^2$. Therefore $4ap = (2am + bn)^2 - dn^2$ and so $dn^2$ is a square mod $4p$. Now $p \nmid n$ else $p | 4ap + dn^2 = (2am + bn)^2$ so that $p | 2am$ which is impossible as $p \nmid 2a$ and $(m, n) = 1$. We deduce that $d$ is a square mod $p$.

(ii) If $d \equiv b^2 \pmod{4p}$ then $d = b^2 - 4pc$ for some integer $c$, and so $px^2 + bxy + cy^2$ is a quadratic form of discriminant $d$ which represents $p = p \cdot 1^2 + b \cdot 1 \cdot 0 + c \cdot 0^2$. \qed
Class number one

**Theorem** Suppose $h(d) = 1$. Then $p$ is represented by the form of discrim $d$ if and only if $d$ is a square mod $4p$.

(Fundamental discriminants: If $q^2 | d$ then $q = 2$ and $d \equiv 8$ or $12 \pmod{16}$.)

The only fundamental $d < 0$ with $h(d) = 1$ are $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$. (Heegner/Baker/Stark)

Euler noticed that the polynomial $x^2 + x + 41$ is prime for $x = 0, 1, 2, \ldots, 39$, and some other polynomials.

**Rabinowicz’s criterion** We have $h(1 - 4A) = 1$ for $A \geq 2$ if and only if $x^2 + x + A$ is prime for $x = 0, 1, 2, \ldots, A - 2$. 
Class number one

Rabinowiscz’s criterion We have $h(1 - 4A) = 1$ for $A \geq 2$ if and only if $x^2 + x + A$ is prime for $x = 0, 1, 2, \ldots, A - 2$.

If $p \nmid d$ then
- $p$ is rep’d by $x^2 + y^2$ if and only if $(-1/p) = 1$,
- $p$ is rep’d by $x^2 + 2y^2$ if and only if $(-2/p) = 1$,
- $p$ is rep’d by $x^2 + xy + y^2$ if and only if $(-3/p) = 1$,
- $p$ is rep’d by $x^2 + xy + 2y^2$ if and only if $(-7/p) = 1$,
- $p$ is rep’d by $x^2 + xy + 3y^2$ if and only if $(-11/p) = 1$,
- $p$ is rep’d by $x^2 + xy + 5y^2$ if and only if $(-19/p) = 1$,
- $p$ is rep’d by $x^2 + xy + 11y^2$ if and only if $(-43/p) = 1$,
- $p$ is rep’d by $x^2 + xy + 17y^2$ if and only if $(-67/p) = 1$,
- $p$ is rep’d by $x^2 + xy + 41y^2$ if and only if $(-163/p) = 1$. 
Class number *not* one

What about when the class number is not one? First example, $h(-20) = 2$, the two reduced forms are $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$.

$p$ is represented by $x^2 + 5y^2$ if and only if $p = 5$, or $p \equiv 1$ or $9 \pmod{20}$;

$p$ is represented by $2x^2 + 2xy + 3y^2$ if and only if $p = 2$, or $p \equiv 3$ or $7 \pmod{20}$.

Cannot always distinguish which primes are represented by which bqf of discriminant $d$ by congruence conditions. Euler found 65 such *idoneal numbers*. No more are known – at most one further idoneal number.
Ideals in quadratic fields

Any ideal $I$ in a quadratic ring of integers:

$$R := \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

is generated by $\leq 2$ elements. If $I \subset \mathbb{Z}$ then principal. Else $\exists r + s\sqrt{d} \in I$ with $s \neq 0$, wlog $s > 0$. Select $s$ minimal.

Claim: If $u + v\sqrt{d} \in I$ then $s$ divides $v$

(else if $ks + \ell v = g := \gcd(s, v)$ then

$(kr + \ell u) + g\sqrt{d} = k(r + s\sqrt{d}) + \ell(u + v\sqrt{d}) \in I \neq$)

Let $v = ms$, so that $(u + v\sqrt{d}) - m(r + s\sqrt{d}) = u - mr$.

Therefore $I = \{m(r + s\sqrt{d}) + n : m \in \mathbb{Z}, n \in I \cap \mathbb{Z}\}$.

Now $I \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$ so principal, $= \langle g \rangle$ say hence

$$I = \langle r + s\sqrt{d}, g \rangle_{\mathbb{Z}}.$$
Any ideal \( I \subset R := \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \) has the form
\[
I = \langle r + s\sqrt{d}, g \rangle_{\mathbb{Z}}.
\]

**More:** \( \sqrt{d} \in R \), so \( g\sqrt{d} \in I \) and \( sd + r\sqrt{d} \in I \), and so
\( s \) divides both \( g \) and \( r \).

Therefore \( r = sb \) and \( g = sa \). Also
\[
s(b^2 - d) = (r + s\sqrt{d})(b - \sqrt{d}) \in I \cap \mathbb{Z}
\]
and so \( s(b^2 - d) \) is a multiple of \( g = sa \); hence \( a \) divides \( b^2 - d \). Therefore
\[
I = s\langle b + \sqrt{d}, a \rangle_{\mathbb{Z}}
\]
for some integers \( s, a, b \) where \( a \) divides \( b^2 - d \).
Binary quadratic forms and Ideals

\[ I = s\langle a, b + \sqrt{d}\rangle_{\mathbb{Z}} \]

If \( f(x, y) = ax^2 + bxy + cy^2 \) then

\[ af(x, y) = \left( ax + \frac{b + \sqrt{d}}{2} y \right) \left( ax + \frac{b - \sqrt{d}}{2} y \right) \]

so we see that \( af(x, y) \) is the Norm of \( \left( ax + \frac{b+\sqrt{d}}{2} y \right) \).

So the set of possible values of \( f(x, y) \) with \( x, y \in \mathbb{Z} \) is in 1-to-1 correspondence with the elements of \( \langle a, \frac{b+\sqrt{d}}{2} \rangle_{\mathbb{Z}} \).
Equivalence of ideals

Any two equivalent bqfs can be obtained from each other by a succession of two basic transformations:

\[ x \rightarrow x+y, \ y \rightarrow y \text{ gives } \langle a, \frac{b + \sqrt{d}}{2} \rangle \mathbb{Z} \rightarrow \langle a, \frac{2a + b + \sqrt{d}}{2} \rangle \mathbb{Z} \]

Now \( \langle a, \frac{b+\sqrt{d}}{2} \rangle \mathbb{Z} = \langle a, \frac{2a+b+\sqrt{d}}{2} \rangle \mathbb{Z} \)

\[ x \rightarrow -y, \ y \rightarrow x \text{ gives } \langle a, \frac{b + \sqrt{d}}{2} \rangle \mathbb{Z} \rightarrow \langle c, \frac{-b + \sqrt{d}}{2} \rangle \mathbb{Z}. \]

Since \( \frac{-b+\sqrt{d}}{2} \cdot \frac{b+\sqrt{d}}{2} = \frac{d-b^2}{4} = -ac \), and therefore

\[ \frac{-b + \sqrt{d}}{2} \cdot \langle a, \frac{b + \sqrt{d}}{2} \rangle \mathbb{Z} = a \cdot \langle \frac{-b + \sqrt{d}}{2}, -c \rangle \mathbb{Z}. \]

So, equivalence of forms, in setting of ideals, gives: For ideals \( I, J \) of \( \mathbb{Q}(\sqrt{d}) \), we have that

\( I \sim J \) if and only there exists \( \alpha \in \mathbb{Q}(\sqrt{d}) \), such that

\( J = \alpha I \).
For ideals $I, J$ of $\mathbb{Q}(\sqrt{d})$, we have that $I \sim J$ if and only there exists $\alpha \in \mathbb{Q}(\sqrt{d})$, such that

$$J = \alpha I.$$  

This works in any number field; moreover then one has finitely many equivalence classes, and $i$ bounds for the “smallest” element of each class.

Any ideal $I = \langle a, \frac{b+\sqrt{d}}{2} \rangle$ with $d < 0$ then we plot $\mathbb{Z}$-linear combinations on the complex plane and they form a lattice, $\Lambda = \langle a, \frac{b+\sqrt{d}}{2} \rangle$ — geometry of lattices.

Equivalence: Two lattices $\Lambda, \Lambda'$ are homothetic if there exists $\alpha \in \mathbb{C}$ such that $\Lambda' = \alpha \Lambda$, and we write $\Lambda' \sim \Lambda$.

Divide through by $a$, every such lattice is homothetic to $\langle 1, \tau \rangle$ where $\tau = \frac{b+\sqrt{d}}{2a}$, in the upper half plane.
**Fundamental discriminants and orders**

A square class of integers, like $3, 12, 27, 48, \ldots$ gives same field $\mathbb{Q}(\sqrt{3n^2}) = \mathbb{Q}(\sqrt{3})$ — minimal one? Candidate: The only one that is squarefree? However, from theory of bqfs need discriminant $\equiv 0$ or $1 \pmod{4}$. Divisibility by 4 correct price to pay. The *fundamental discriminant* of a quadratic field to be the smallest element of the square class of the discriminant which is $\equiv 0$ or $1 \pmod{4}$. For $d$ squarefree integer, the fundamental discriminant $D$ is

$$D = \begin{cases} d & \text{if } d \equiv 1 \pmod{4} \\ 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \end{cases}.$$ 

The ring of integers is $\mathbb{Z} \left[ \frac{D + \sqrt{D}}{2} \right]$ or $\mathbb{Z}[\omega] = \langle 1, \omega \rangle_{\mathbb{Z}}$,

$$\omega := \begin{cases} \frac{1 + \sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4} \\ \sqrt{d} = \sqrt{D}/2 & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \end{cases}.$$
Gauss’s Composition Law

The product of any two values of a principal form gives a third value of that quadratic form:

\[(a^2 + db^2)(c^2 + de^2) = (ac + dbe)^2 + d(ae - bc)^2.\]

Gauss: if \(f\) and \(g\) are bqfs discrim \(d\), then \(\exists\) bqf \(h\) of discrim \(d\), such that any

\[f(a, b)g(c, e) = h(m, n),\]

\[m = m(a, b, c, e), \quad n = n(a, b, c, e)\]

are bilinear forms. Gauss showed this explicitly via formulae; e.g., for three bqfs of discrim \(-71\),

\[2m^2 + mn + 9n^2 = (4a^2 + 3ab + 5b^2)(3c^2 + ce + 6e^2).\]

with \(m = ac - 3ae - 2bc - 3be\) and \(n = ac + ae + bc - be\).

Gauss called this composition.
\[2m^2 + mn + 9n^2 = (4a^2 + 3ab + 5b^2)(3c^2 + ce + 6e^2).\]

Gauss showed composition stays consistent under the equivalence relation.

Allows us to find a group structure on the classes of quadratic forms of given discriminant, the \textit{class group}.

Gauss’s proof is monstrously difficult, even in the hands of the master the algebra involved is so overwhelming that he does not include many details.

Gauss’s student \textbf{Dirichlet} found several ways to simplify composition. The first involved finding forms that are equivalent to \(f\) and \(g\) that are easier to compose:
Dirichlet’s composition of forms

• For any given integer \( w \) there exist integers \( m, n \) with \((am^2 + bmn + cn^2, w) = 1\).

• Given quadratic forms \( f \) and \( g \), find \( f' \sim f \) such that \((f'(1, 0), g(1, 0)) = 1\).

• There exists \( F \sim f' \) and \( G \sim g \) such that \( F(x, y) = ax^2 + bxy + cy^2 \) and \( G(x, y) = Ax^2 + bxy + Cy^2 \) with \((a, A) = 1\).

• If \( f \) and \( g \) have the same discriminant then there exist \( h \) such that \( F(x, y) = ax^2 + bxy + Ahy^2 \) and \( G(x, y) = Ax^2 + bxy + ah y^2 \) with \((a, A) = 1\).

• \( d = b^2 - 4aAh \). If \( H(x, y) = aAx^2 + bxy + hy^2 \) then

\[
\begin{align*}
H(ux - hvy, auy + Avx + bvy) &= F(u, v)G(x, y)
\end{align*}
\]
Dirichlet’s composition of ideals

Dirichlet simplified by defining ideals: To multiply two ideals, $IJ = \{ij : i \in I, j \in J\}$.

$$2m^2 + mn + 9n^2 = (4a^2 + 3ab + 5b^2)(3c^2 + ce + 6e^2).$$

$$(4, \frac{3+\sqrt{-71}}{2})$$ corresponds to $4a^2 + 3ab + 5b^2$, and

$$(3, \frac{1+\sqrt{-71}}{2})$$ corresponds to $3c^2 + ce + 6e^2$. Then

$$\left(4, \frac{3+\sqrt{-71}}{2}\right) \left(3, \frac{1+\sqrt{-71}}{2}\right) = \left(12, \frac{-5+\sqrt{-71}}{2}\right),$$

which corresponds to $12x^2 - 5xy + 2y^2$, also of disc $-71$, but not reduced. Reduction then yields:

$$(12, -5, 2) \sim (2, 5, 12) \sim (2, 1, 9)$$
Comparing Dirichlet’s compositions

If \( F = ax^2 + bxy + Ahy^2 \), \( G = Ax^2 + bxy + ah^2 \) then

\[
H(ux - hvy, auy + Avx + bvy) = F(u, v)G(x, y)
\]

for \( H(x, y) = aAx^2 + bxy + hy^2 \).

The two quadratic forms \( F \) and \( G \) correspond to \( (a, \frac{-b + \sqrt{d}}{2}) \) and \( (A, \frac{-b + \sqrt{d}}{2}) \). The product is \( (aA, \frac{-b + \sqrt{d}}{2}) \), so the composition of \( F \) and \( G \) must be \( aAx^2 + bxy + hy^2 \).

Identity of ideal class group: principal ideas. Inverses:

\[
\left( a, \frac{b + \sqrt{d}}{2} \right) \left( a, \frac{b - \sqrt{d}}{2} \right) = \left( a^2, a \cdot \frac{b + \sqrt{d}}{2}, a \cdot \frac{b - \sqrt{d}}{2}, \frac{b^2 - d}{4} \right)
\]

\[\supseteq a (a, b, c) = (a),\]

So an ideal and its conjugate are inverses in class group.
A more general set up

Let \( G(\mathbb{Z}) \) be \( \text{SL}(2, \mathbb{Z}) \), an “algebraic group”; \( V(\mathbb{Z}) \) the space of bqfs over \( \mathbb{Z} \), a “representation”. Seen that: The \( G(\mathbb{Z}) \)-orbits parametrize the ideal classes in the associated quadratic rings.

Do other such pairs exist? That is an algebraic group \( G \) and associated representation \( V \) such that \( G(\mathbb{Z}) \setminus V(\mathbb{Z}) \) parametrizes something interesting? Eg rings, modules etc of arithmetic interest.

In our example there is just one orbit over \( \mathbb{C} \):

**A pre-homogenous vector space** is a pair \((G, V)\) where \( G \) is an algebraic group and \( V \) is a rational vector space representation of \( G \) such that the action of \( G(\mathbb{C}) \) on \( V(\mathbb{C}) \) has just one Zariski open orbit.
A pre-homogenous vector space is a pair \((G, V)\) where \(G\) is an algebraic group and \(V\) is a rational vector space representation of \(G\) such that the action of \(G(\mathbb{C})\) on \(V(\mathbb{C})\) has just one Zariski open orbit.

Bhargava’s program centres around study of \(G(\mathbb{Z}) \setminus V(\mathbb{Z})\) for pre-homogenous vector spaces \((G, V)\).

There are just 36 of them (Sato-Kimura, 1977), but they have proved to be incredibly rich in structure of interest to number theorists.
Bhargava composition

Recently Bhargava gave a new insight into the composition law.

Note: If $IJ = K$ then $IJK$ is principal.
Bhargava composition

We begin with a 2-by-2-by-2 cube. \( a, b, c, d, e, f, g, h \). Six faces, can be split into three parallel pairs. To each consider pair of 2-by-2 matrices by taking the entries in each face, with corresponding entries corresponding to opposite corners of the cube, always starting with \( a \). Hence we get the pairs

\[
M_1(x, y) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} x + \begin{pmatrix} e & f \\ g & h \end{pmatrix} y,
\]

\[
M_2(x, y) := \begin{pmatrix} a & c \\ e & g \end{pmatrix} x + \begin{pmatrix} b & d \\ f & h \end{pmatrix} y,
\]

\[
M_3(x, y) := \begin{pmatrix} a & b \\ e & f \end{pmatrix} x + \begin{pmatrix} c & d \\ g & h \end{pmatrix} y,
\]

where we have, in each added the dummy variables, \( x, y \). The determinant, \(-Q_j(x, y)\), of each \( M_j(x, y) \) gives rise to a quadratic form in \( x \) and \( y \).
$M_1(x, y) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} x + \begin{pmatrix} e & f \\ g & h \end{pmatrix} y,$

$M_2(x, y) := \begin{pmatrix} a & c \\ e & g \end{pmatrix} x + \begin{pmatrix} b & d \\ f & h \end{pmatrix} y,$

$M_3(x, y) := \begin{pmatrix} a & b \\ e & f \end{pmatrix} x + \begin{pmatrix} c & d \\ g & h \end{pmatrix} y,$

$Q_j(x, y) = - \det M_j(x, y), \text{ a bqf}$

Now apply an $\text{SL}(2, \mathbb{Z})$ transformation in one direction. That is, if $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$ then we replace the face

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \beta$

and

$\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \delta.$
$M_1(x, y) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} x + \begin{pmatrix} e & f \\ g & h \end{pmatrix} y,$

If $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$ then we replace the face

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \beta$

and

$\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \delta.$

Then $M_1(x, y)$ gets mapped to

$\begin{cases} \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \beta \right) x + \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \delta \right) y, \end{cases}$

that is $M_1(\alpha x + \gamma y, \beta x + \delta y)$. Therefore

$Q_1(x, y) = - \det M_1(x, y)$ gets mapped to

$Q_1(\alpha x + \gamma y, \beta x + \delta y).$ which is equivalent to $Q_1(x, y).$
Now $M_2(x, y)$ gets mapped to

$$\begin{pmatrix} a\alpha + e\beta & c\alpha + g\beta \\ a\gamma + e\delta & c\gamma + g\delta \end{pmatrix} x + \begin{pmatrix} b\alpha + f\beta & d\alpha + h\beta \\ b\gamma + f\delta & d\gamma + h\delta \end{pmatrix} y$$

$$= \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} M_2(x, y);$$

hence the determinant, $Q_2(x, y)$, is unchanged. An analogous calculation reveals that $M_3(x, y)$ gets mapped to

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} M_3(x, y)$$

and its det, $Q_3(x, y)$ also unchanged.

Therefore we can act on our cube by such SL(2, $\mathbb{Z}$)-transformations, in each direction, and each of the three quadratic forms remains in the same equivalence class.
Another prehomogenous vector space

We can act on our cube by such $\text{SL}(2, \mathbb{Z})$-transformations, in each direction, and each of the three quadratic forms remains in the same equivalence class.

Bhargava’s cubes can be identified as

$$a \ e_1 \times e_1 \times e_1 + b \ e_1 \times e_2 \times e_1 + c \ e_2 \times e_1 \times e_1 + d \ e_2 \times e_2 \times e_1 + e \ e_1 \times e_1 \times e_2 + f \ e_1 \times e_2 \times e_2 + g \ e_2 \times e_1 \times e_2 + h \ e_2 \times e_2 \times e_2$$

with

the representation $\mathbb{Z}^2 \times \mathbb{Z}^2 \times \mathbb{Z}^2$

of the group

$\text{SL}(2, \mathbb{Z}) \times \text{SL}(2, \mathbb{Z}) \times \text{SL}(2, \mathbb{Z})$.

This pair is also a prehomogenous vector space
Reducing a Bhargava cube

Simplify entries using the following reduction algorithm:

• We select the corner that is to be \( a \) so that \( a \neq 0 \).
• Transform cube to ensure \( a \) divides \( b, c \) and \( e \).

If not, say \( a \) does not divide \( e \), n select integers \( \alpha, \beta \) so that \( a\alpha + e\beta = (a, e) \). Let \( \gamma = -e/(a, e) \), \( \delta = a/(a, e) \).

In transformed matrix

\[
a' = (a, e), \quad e' = 0 \quad \text{and} \quad 1 \leq a' \leq a - 1.
\]

If \( a' \) does not divide \( b' \) or \( c' \), repeat the process.

Each time we reduce \( a \), so a finite process.

• Transform cube to ensure \( b = c = e = 0 \). Select \( \alpha = 1, \beta = 0, \gamma = -e/a, \delta = 1 \), so that \( e' = 0, b' = b, c' = c \). We repeat this in each of the three directions to ensure that \( b = c = e = 0 \).
Reducing a Bhargava cube, II

Replacing \(a\) by \(-a\), we have that the three matrices are:

\[
M_1 = \begin{pmatrix} -a & 0 \\ 0 & d \end{pmatrix} x + \begin{pmatrix} 0 & f \\ g & h \end{pmatrix} y, \quad \text{so} \quad Q_1 = adx^2 + ahxy + fgy^2;
\]
\[
M_2 = \begin{pmatrix} -a & 0 \\ 0 & g \end{pmatrix} x + \begin{pmatrix} 0 & d \\ f & h \end{pmatrix} y, \quad \text{so} \quad Q_2 = agx^2 + ahxy + dfy^2;
\]
\[
M_3 = \begin{pmatrix} -a & 0 \\ 0 & f \end{pmatrix} x + \begin{pmatrix} 0 & d \\ g & h \end{pmatrix} y, \quad \text{so} \quad Q_3 = afx^2 + ahxy + dgy^2.
\]

All \(\text{discrim}(Q_j) = (ah)^2 - 4adf g\), and

\(Q_1(fy_2x_3 + gx_2y_3 + hy_2y_3, ax_2x_3 - dy_2y_3) = Q_2(x_2, y_2)Q_3(x_3, y_3)\)

\(x_1 = fy_2x_3 + gx_2y_3 + hy_2y_3\) and \(y_1 = ax_2x_3 - dy_2y_3\).

Dirichlet: \(a = 1\). So

Includes every pair of bqfs of same discriminant.
Pre-homogenous vector spaces

**SL(2, \mathbb{Z})**-transformations. Forms-Ideals-Transformations

**Generators of** \( SL(2, \mathbb{Z}) \), \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \). correspond to two basic ops in Gauss’s reduction algorithm

The first is \( x \to x + y, y \to y \), so that

\[
 f(x, y) \sim g(x, y) := f(x+y, y) = ax^2 + (b+2a)xy + (a+b+c)y^2.
\]

Note that \( I_g = (2a, -(b + 2a) + \sqrt{d}) = I_f \),

and \( z_g = \frac{-b-2a+\sqrt{d}}{2a} = z_f - 1 \).
Generators of $\text{SL}(2, \mathbb{Z})$ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. correspond to two basic ops in Gauss’s reduction algorithm. The first is $x \to x + y, y \to y$, so that

$$f(x, y) \sim g(x, y) := f(x+y, y) = ax^2 + (b+2a)xy + (a+b+c)y^2.$$  

Note that $I_g = (2a, -(b + 2a) + \sqrt{d}) = I_f$, and $z_g = \frac{-b-2a+\sqrt{d}}{2a} = z_f - 1$.

The second is $x \to y, y \to -x$ so that

$$f(x, y) \sim h(x, y) := f(y, -x) = cx^2 - bxy + ay^2.$$  

Note that $I_h = (2c, b + \sqrt{d})$, and $z_h = \frac{b+\sqrt{d}}{2c}$.

$$z_f \cdot z_h = \frac{-b+\sqrt{d}}{2a} \cdot \frac{b+\sqrt{d}}{2c} = \frac{d - b^2}{4ac} = -1$$  

that is $z_h = -1/z_f$. Then

$$I_h \sim (1, z_h) = (1, -1/z_f) \sim (1, -z_f) = (1, z_f) \sim I_f.$$
Since any $\text{SL}(2, \mathbb{Z})$-transformation can be constructed out of the basic two transformation we deduce

**Theorem** $f \sim f'$ if and only if $I_f \sim I_{f'}$ if and only if $z_f \sim z_{f'}$. 
The ring of integers of a quadratic field, revisited

Integer solutions $x, y$ to $x^2 + 19 = y^3$?

If so, $y$ is odd else $x^2 \equiv 5 \pmod{8}$. Also $19 \nmid y$ else $19 | x \implies 19 \equiv x^2 + 19 = y^3 \equiv 0 \pmod{19^2}$.

Hence $(y, 38) = 1$.

Now $(x + \sqrt{-19})(x - \sqrt{-19}) = y^3$ and $(x + \sqrt{-19}, x - \sqrt{-19})$ contains $2\sqrt{-19}$ and $y^3$.

Hence the ideals $(x + \sqrt{-19})$ and $(x - \sqrt{-19})$ are coprime.

Their product is a cube and so they are both cubes.
Integer solutions $x, y$ to $x^2 + 19 = y^3$ ?

The ring of integers of $\mathbb{Q}[\sqrt{-19}]$ has class number one. So every ideal is principal. Hence

$$x + \sqrt{-19} = u(a + b\sqrt{-19})^3 \text{ where } u \text{ is a unit.}$$

Only units: 1 and $-1$. Change $a, b$, to $ua, ub$. Hence

$$x + \sqrt{-19} = (a + b\sqrt{-19})^3$$

$$= a(a^2 - 57b^2) + b(3a^2 - 19b^2)\sqrt{-19},$$

so that $b(3a^2 - 19b^2) = 1$.

Therefore $b = \pm 1$ and so $3a^2 = 19b^2 \pm 1 = 19 \pm 1$ which is impossible. We deduce:

*There are no integer solutions $x, y$ to $x^2 + 19 = y^3$."

*However* what about $18^2 + 19 = 7^3$?

The mistake: The ring of integers of $\mathbb{Q}[\sqrt{-19}]$ is *not* the set of numbers of the form $a + b\sqrt{-19}$ with $a, b \in \mathbb{Z}$. *It is* $(a + b\sqrt{-19})/2$ with $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{2}$. 
Integer solutions \( x, y \) to \( x^2 + 19 = y^3 \) ?

The ring of integers of \( \mathbb{Q}[\sqrt{-19}] \) has class number one. So every ideal is principal. Hence

\[
x + \sqrt{-19} = (\frac{a+b\sqrt{-19}}{2})^3
\]

\[
8x + 8\sqrt{-19} = (a + b\sqrt{-19})^3
\]

\[
= a(a^2 - 57b^2) + b(3a^2 - 19b^2)\sqrt{-19},
\]

so that \( b(3a^2 - 19b^2) = 8 \). Therefore

\( b = \pm 1, \pm 2, \pm 4 \) or \( \pm 8 \) and so

\( 3a^2 = 19 \pm 8, 19 \cdot 4 \pm 4, 19 \cdot 16 \pm 2 \) or \( 19 \cdot 64 \pm 1 \).

The only solution is \( b = 1, a = \pm 3 \) leading to

\( x = \mp 18, y = 7 \), the only solutions.