MAU23101 Introduction to number theory
5 - Binary quadratic forms

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2020–2021
Version: November 18, 2020

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Representation by forms

Forms (non examinable)

Definition

A form is a homogeneous polynomial (all terms have the same total degree)

Example

$F(x,y,z) = 2x^5 - 7xy^3z + xyz^3 - 9y^4z$ is a ternary quintic form.
Ternary: 3 variables x,y,z.
Quintic: Total degree 5.

In this chapter, we study binary quadratic forms.
Binary: 2 variables x,y.
Quadratic: Total degree 2.

$$\rightsquigarrow F(x,y) = Ax^2 + Bxy + Cy^2, \quad A,B,C \in \mathbb{Z}.$$

Representation by a form

Definition ((Proper) representation)

Let $F(x,y) = Ax^2 + Bxy + Cy^2$ be a form, and let $n \in \mathbb{Z}$.

- *F represents n if there exist $r, s \in \mathbb{Z}$ such that $n = F(r,s)$.*
- *F properly represents n if there exist $r, s \in \mathbb{Z}$ such that $n = F(r,s)$ and $\gcd(r,s) = 1$.*

Remark

$F(dr, ds) = A(dr)^2 + B(dr)(ds) + C(ds)^2 = d^2 F(r,s)$, so
F represents $n \iff n = d^2 m$, $d \in \mathbb{N}$, m properly rep. by F.

Representation by a form

Definition ((Proper) representation)

Let $F(x,y) = Ax^2 + Bxy + Cy^2$ be a form, and let $n \in \mathbb{Z}$.

- *F represents n if there exist $r, s \in \mathbb{Z}$ such that $n = F(r,s)$.*
- *F properly represents n if there exist $r, s \in \mathbb{Z}$ such that $n = F(r,s)$ and $\gcd(r,s) = 1$.*

Definition (Primitive form)

$F(x,y) = Ax^2 + Bxy + Cy^2$ is primitive if $\gcd(A,B,C) = 1$.

Remark

Let $g = \gcd(A,B,C)$.
Then $F(x,y) = gF_1(x,y)$, where $F_1(x,y)$ is primitive, and F (properly) represents $gn \iff F_1$ (properly) represents n.

Representation by a form

Definition ((Proper) representation)

Let $F(x,y) = Ax^2 + Bxy + Cy^2$ *be a form, and let* $n \in \mathbb{Z}$.

- F *represents* n *if there exist* $r,s \in \mathbb{Z}$ *such that* $n = F(r,s)$.
- F *properly represents* n *if there exist* $r,s \in \mathbb{Z}$ *such that* $n = F(r,s)$ *and* $\gcd(r,s) = 1$.

Definition (Primitive form)

$F(x,y) = Ax^2 + Bxy + Cy^2$ *is primitive if* $\gcd(A,B,C) = 1$.

$\rightsquigarrow$ We focus on proper representation by primitive forms.

Example

$F(x,y) = x^2 + y^2$ is primitive. For all $p \in \mathbb{N}$ prime,
F rep. $p \iff F$ prop. rep. $p \iff p \not\equiv -1 \bmod 4$.

Equivalence and discriminant

Discriminant

Definition

The discriminant of $F(x,y) = Ax^2 + Bxy + Cy^2$ *is*

$$\Delta_F = B^2 - 4AC.$$

Remark

Mod 4, $\Delta_F \equiv B^2 \equiv \begin{cases} 0 & \text{if } B \text{ even,} \\ 1 & \text{if } B \text{ is odd.} \end{cases}$

Conversely, any integer $\equiv 0$ or 1 mod 4 is a discriminant.

Discriminant

Definition

The <u>discriminant</u> of $F(x,y) = Ax^2 + Bxy + Cy^2$ *is*

$$\Delta_F = B^2 - 4AC.$$

Remark

$4AF(x,y) = (2Ax + By)^2 - \Delta_F y^2$, so

- If $\Delta_F > 0$, then F represents integers of both signs.
- If $\Delta_F < 0$, then A and C have the same sign, and F only represents integers of that sign.
- If $\Delta_F = 0$, then F only represents squares times A.

Example

$F(x,y) = x^2 + y^2$ has $\Delta_F = -4$, so it only reps. integers > 0.
$G(x,y) = 2x^2 + 5xy + y^2$ has $\Delta_G = 17$, so it reps. both signs.

Equivalence of forms, 1/3

Clearly $F(x,y)$ and $F(y,x)$ represent the same integers.

Same for $F(x,y)$ and $F(2x+y,x+y)$, since if $x'=2x+y$ and $y'=x+y$, then $x=x'-y'$ and $y=2y'-x'$.

But (probably) not so for $F(x,y)$ and $F(2x-y,x+y)$, since if $x'=2x-y$ and $y'=x+y$, then $x=\frac{x'+y'}{3}$ and $y=\frac{2y'-x'}{3}$.

$\rightsquigarrow$ We could allow changes of variables of the form

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}$$

where M is a 2×2 matrix with coefficients in $\mathbb{Z}$, which is invertible, and whose inverse also has coefficients in $\mathbb{Z}$.

Definition

$\mathrm{GL}_2(\mathbb{Z}) = \{M \in \mathcal{M}_{2\times 2}(\mathbb{Z}) \mid M \text{ invertible and } M^{-1} \in \mathcal{M}_{2\times 2}(\mathbb{Z})\}$.

Theorem

Let $M \in \mathcal{M}_{2\times 2}(\mathbb{Z})$. Then
$M \in \mathrm{GL}_2(\mathbb{Z}) \iff \det M \in \mathbb{Z}^\times \iff \det M = \pm 1$.

Proof.

$\Rightarrow$: If $M \in \mathrm{GL}_2(\mathbb{Z})$, then $MM^{-1} = I_2$, so
$1 = \det(I_2) = \det(MM^{-1}) = \underbrace{\det(M)}_{\in\mathbb{Z}}\underbrace{\det(M^{-1})}_{\in\mathbb{Z}}$.

$\Leftarrow$: If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z})$ has $ad - bc = \pm 1$, then

$$M^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}).$$

□

Equivalence of forms, 2/3

Theorem

Let $M \in \mathcal{M}_{2\times 2}(\mathbb{Z})$. Then
$M \in \mathrm{GL}_2(\mathbb{Z}) \iff \det M \in \mathbb{Z}^\times \iff \det M = \pm 1$.

Proof.

$\Rightarrow$: If $M \in \mathrm{GL}_2(\mathbb{Z})$, then $MM^{-1} = I_2$, so
$1 = \det(I_2) = \det(MM^{-1}) = \underbrace{\det(M)}_{\in\mathbb{Z}}\underbrace{\det(M^{-1})}_{\in\mathbb{Z}}$.

$\Leftarrow$: If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z})$ has $ad - bc = \pm 1$, then

$$M^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}).$$

□

Remark

This is not specific to size 2×2, nor to $\mathbb{Z}$.

Equivalence of forms, 3/3

Definition

Two forms F_1 and F_2 are equivalent, written $F_1 \sim F_2$, if

$$F_2(x,y) = F_1(ax+cy, bx+dy)$$

with $a,b,c,d \in \mathbb{Z}$, $ad-bc=+1$.

In other words, we only allow changes of variables induced by

$$M \in \mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a,b,c,d \in \mathbb{Z},\ ad-bc=+1 \right\}.$$

Remark

Then $F_1(x,y) = F_2(dx-cy, -bx+ay)$, so $F_2 \sim F_1$.
Besides, $F_1 \sim F_1$; and if $F_1 \sim F_2 \sim F_3$, then $F_1 \sim F_3$.
So this really is an equivalence relation.

Equivalence of forms, 3/3

Definition

Two forms F_1 and F_2 are equivalent, written $F_1 \sim F_2$, if

$$F_2(x,y) = F_1(ax+cy, bx+dy)$$

with $a,b,c,d \in \mathbb{Z}$, $ad-bc = +1$.

Proposition

If $F_1 \sim F_2$, then F_1 and F_2 represent the same integers, and properly represent the same integers.

Proof.

Let $r,s \in \mathbb{Z}$, $M \in \mathrm{GL}_2(\mathbb{Z})$, and $\begin{pmatrix} r' \\ s' \end{pmatrix} = M \begin{pmatrix} r \\ s \end{pmatrix}$. As $\begin{pmatrix} r \\ s \end{pmatrix} = M^{-1} \begin{pmatrix} r' \\ s' \end{pmatrix}$,

if $d \mid r,s$, then $d \mid r',s'$ and vice versa.

Thus $\gcd(r',s') = \gcd(r,s)$. $\square$

Equivalence of forms, 3/3

Definition

Two forms F_1 and F_2 are equivalent, written $F_1 \sim F_2$, if

$$F_2(x,y) = F_1(ax+cy, bx+dy)$$

with $a,b,c,d \in \mathbb{Z}$, $ad - bc = +1$.

Proposition

If $F_1 \sim F_2$, then $\Delta_{F_1} = \Delta_{F_2}$.

Proof.

Calculation. □

Lemmas: Representation vs. equivalence

Representation vs. equivalence

Lemma

Let $F(x,y)$ be a form, and let $n \in \mathbb{Z}$. Then F properly represents $n \iff F \sim nx^2 + Bxy + Cy^2$ for some $B, C \in \mathbb{Z}$.

Proof.

$\Leftarrow$: The form $nx^2 + Bxy + Cy^2$ prop. reps. n by $x = 1$, $y = 0$.

$\Rightarrow$: Suppose $F(r,s) = n$, with $r, s \in \mathbb{Z}$ and $\gcd(r,s) = 1$. Bézout $\rightsquigarrow$ there are $u, v \in \mathbb{Z}$ such that $ru + sv = 1$. Thus $M = \begin{pmatrix} r & -v \\ s & u \end{pmatrix}$ has $\det M = +1$, and turns $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ into $\begin{pmatrix} r \\ s \end{pmatrix}$. Let $F' = A'x^2 + B'xy + C'y^2$ be the equivalent form obtained by applying M^{-1} to F; then $A' = F'(1,0) = F(r,s) = n$. $\square$

Representation vs. equivalence

Theorem

Let $D \in \mathbb{Z}$ be $\equiv 0$ or $1 \bmod 4$, and let $n \in \mathbb{Z}$ be odd and coprime to D. Then n is properly represented by a primitive form of discriminant $D \iff D$ is a square mod n.

Proof.

$\Rightarrow$: Suppose F has $\Delta_F = D$ and prop. represents n. By lemma, $F \sim F' = nx^2 + Bxy + Cy^2$, whence
$D = \Delta_F = \Delta_{F'} = B^2 - 4nC \equiv B^2 \bmod n$.

$\Leftarrow$: $D \equiv B^2 \bmod n$ for some $B \in \mathbb{Z}$. Replacing B with $B + n$ if necessary, WLOG $B \equiv D \bmod 2$, whence $B^2 \equiv D \bmod 4$, so $B^2 \equiv D \bmod 4n$ by CRT. Thus $B^2 = D + 4nC$ for some $C \in \mathbb{Z}$, and then $F = nx^2 + Bxy + Cy^2$ has $\Delta_F = D$, prop. reps. n, and is primitive since
$d \mid n, B \Rightarrow d \mid (B^2 - 4nC) = D$ yet $\gcd(n, D) = 1$. □

Representation vs. equivalence

Theorem

Let $D \in \mathbb{Z}$ be $\equiv 0$ or $1 \bmod 4$, and let $n \in \mathbb{Z}$ be odd and coprime to D. Then n is properly represented by a primitive form of discriminant $D \iff D$ is a square mod n.

Corollary

Let $D \in \mathbb{Z}$ be 0 or $1 \bmod 4$, and let $p \nmid D$ be a prime $\neq 2$. Then p is represented by a form of discriminant $D \iff \left(\frac{D}{p}\right) = +1$.

Reduced forms

Reduced forms

From now on, we only consider primitive forms

$$F(x,y) = Ax^2 + Bxy + Cy^2$$

with $\Delta_F < 0$ and $A, C > 0$.

Definition

Such a form is reduced if $|B| \leq A \leq C$, and if furthermore $B \geq 0$ if $|B| = A$ or if $A = C$.

Theorem

Every form is equivalent to a unique reduced form.

Example

The forms $2x^2 + xy + 4y^2$ and $2x^2 - xy + 4y^2$ are both reduced, so they are not equivalent, even though they (properly) represent the same integers!

Proof of existence

Let $F(x,y) = Ax^2 + Bxy + Cy^2$. We first achieve $|B| \leqslant A \leqslant C$:

- If $A > C$, then $F(x,y) \underset{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)}{\sim} F(y,-x) = Cx^2 - Bxy + Ay^2$.
- Let $m \in \mathbb{Z}$ such that $\left|\frac{B}{2A} - m\right| \leqslant \frac{1}{2}$; then $|B - 2Am| \leqslant A$, and $F(x,y) \underset{\left(\begin{smallmatrix} 1 & -m \\ 0 & 1 \end{smallmatrix}\right)}{\sim} F(x-my,y) = Ax^2 + (B-2Am)xy + C'y^2$.

Along this process, $A \in \mathbb{N}$ keeps decreasing, so this must end.

Then we deal with the special cases:

- If $A = -B$, then
$$F(x,y) = Ax^2 - Axy + Cy^2 \underset{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)}{\sim} F(x+y,y) = Ax^2 + Axy + Cy^2.$$
- If $A = C$, then
$$F(x,y) = Ax^2 - Bxy + Ay^2 \underset{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)}{\sim} F(y,-x) = Ax^2 + Bxy + Ay^2.$$

Example of reduction

Let $F(x,y) = 11x^2 - 50xy + 57y^2$.

$\frac{-50}{2\times 11} = -2.27\cdots \approx -2$, so

$$F(x,y) \underset{\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)}{\sim} F(x+2y,y) = 11x^2 - 6xy + y^2 = F_1(x,y).$$

$11 > 1$, so

$$F_1(x,y) \underset{\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)}{\sim} F_1(y,-x) = x^2 + 6xy + 11y^2 = F_2(x,y).$$

$\frac{6}{2\times 1} = 3$, so

$$F_2(x,y) \underset{\left(\begin{smallmatrix}1 & -3\\ 0 & 1\end{smallmatrix}\right)}{\sim} F_2(x-3y,y) = x^2 + 2y^2.$$

This is reduced, so we stop: $F(x,y) \sim x^2 + 2y^2$.

Geometric interpretation (non examinable)

To $F(x,y) = Ax^2 + Bxy + Cy^2$,
we attach the root

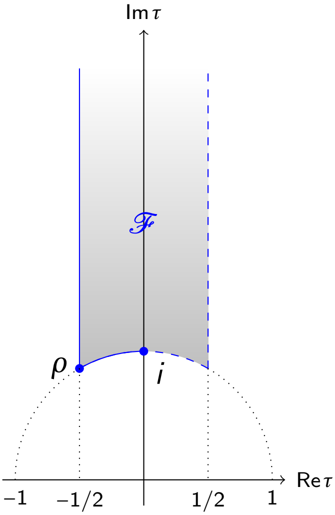
$$\tau = \frac{-B + i\sqrt{-D}}{2A}$$

of $F(x,1) = 0$ such that $\operatorname{Im}\tau > 0$.

We have $\operatorname{Re}\tau = \frac{-B}{2A}$ and $|\tau|^2 = \tau\overline{\tau} = \frac{C}{A}$,
so $|B| \leq A \leq C \iff |\operatorname{Re}\tau| \leq \frac{1}{2}$, $|\tau| \geq 1$.

Thus $F(x,y)$ is reduced $\iff \tau \in \mathscr{F}$.

Besides, $F(x,y) = A(x - y\tau)(x - y\overline{\tau})$
is determined by τ as it is primitive.



Geometric interpretation (non examinable)

Lemma

For all $\tau \in \mathbb{C} \setminus \mathbb{R}$ and $a, b, c, d \in \mathbb{R}$ such that $c, d \neq 0$,

$$\operatorname{Im} \frac{a\tau + b}{c\tau + d} = \frac{(ad - bc) \operatorname{Im} \tau}{|c\tau + d|^2}.$$

Lemma

Hitting $F(x, y)$ with the change of variables corresponding to $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ amounts to replacing τ with $\frac{a\tau+b}{c\tau+d}$.

Let $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.
Then $S : \tau \mapsto -1/\tau$ exchanges the inside and the outside of the circle, and for each $m \in \mathbb{Z}$, $T^m = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right) : \tau \mapsto \tau + m$ is the horizontal translation by m.
The reduction algorithm means that any $\tau \in \mathbb{C}$, $\operatorname{Im} \tau > 0$ can be brought into $\mathscr{F}$ by the action of S and T.

Proof of uniqueness (non examinable)

Suppose $F \underset{M}{\sim} F'$ are both reduced, where $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.
We want to show that $F = F'$, or alternatively that $\tau = \tau'$.

Both τ and $\tau' = \frac{a\tau+b}{c\tau+d}$ lie in $\mathscr{F}$. WLOG $\operatorname{Im}\tau \leq \operatorname{Im}\tau' = \frac{\operatorname{Im}\tau}{|c\tau+d|^2}$, so

$$1 \geq |c\tau+d|^2 = c^2|\tau|^2 + 2cd\operatorname{Re}\tau + d^2 \geq c^2 - |cd| + d^2.$$

Expanding $(c \pm d)^2 \geq 0$ yields $\mp 2cd \leq c^2 + d^2$, whence $|cd| \leq \frac{c^2+d^2}{2}$. So we have $1 \geq \frac{c^2+d^2}{2}$ and therefore $|c| \leq 1$.

Proof of uniqueness (non examinable)

$M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$; both τ and $\tau' = \frac{a\tau+b}{c\tau+d}$ lie in $\mathscr{F}$.

WLOG $\operatorname{Im}\tau \leq \operatorname{Im}\tau' \rightsquigarrow |c\tau + d| \leq 1 \rightsquigarrow c \in \{0, \pm 1\}$.

If $c = 0$, then $1 = \det M = ad$ so $a = d = \pm 1$. Thus $\tau' = \tau \pm b$
$\rightsquigarrow b = 0$, $M = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $F' = F$.

Proof of uniqueness (non examinable)

$M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$; both τ and $\tau' = \frac{a\tau+b}{c\tau+d}$ lie in $\mathscr{F}$.

WLOG $\operatorname{Im}\tau \leq \operatorname{Im}\tau' \rightsquigarrow |c\tau+d| \leq 1 \rightsquigarrow c \in \{0, \pm 1\}$.

If $c = \pm 1$, then WLOG $c = 1$ (replace M with $-M$). Then $|\tau + d| \leq 1$, so $d = 0$, unless $\tau = \rho$ and $d = 1$.

- If $d = 1$, then $1 = \det M = a - b$, so $\tau' = \frac{a\rho+(a-1)}{\rho+1} = a - \frac{1}{\rho+1} = a + \rho$ since $\rho^2 + \rho + 1 = 0$. Thus $a = 0$ and $\tau' = \tau = \rho$, so $F' = F = x^2 + xy + y^2$.
- If $d = 0$, then $|\tau| \leq 1$ so $|\tau| = 1$ thus $|\tau'| = 1$. Besides, $1 = \det M = -b$. Thus $\tau' = \frac{a\tau-1}{\tau} = a - \frac{1}{\tau} = a - \overline{\tau}$. Since $\tau, \tau \in \mathscr{F}$, real parts show that either $\tau = i$ and $a = 0$, or $\tau = \rho$ and $a = -1$. Either way, $\tau' = \tau$, so $F' = F$. $\square$

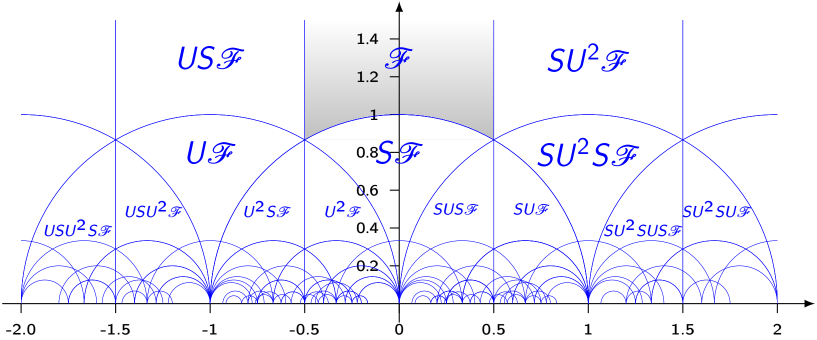
Proof of uniqueness (non examinable)

Remark

We have shown that the translates of $\mathscr{F}$ under $\mathrm{SL}_2(\mathbb{Z})/\pm 1$ tesselate the upper half-plane. For this reason, $\mathscr{F}$ is called a fundamental domain.

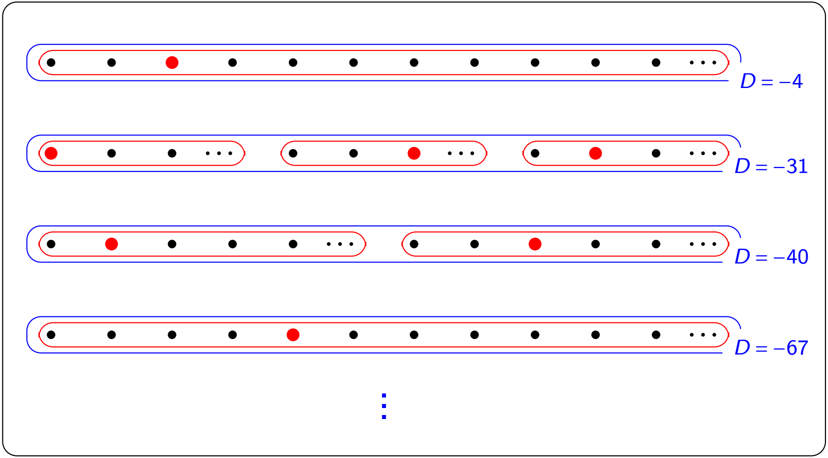
This also shows that $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \rangle$, and even that

$$\mathrm{SL}_2(\mathbb{Z})/\pm 1 \underset{U=T^{-1}S}{=} \langle S, U \mid S^2 = U^3 = 1 \rangle \simeq (\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z}).$$



The class number

Summary: Classification of positive definite forms



• Form

● Reduced form


Forms of the same discriminant


Equivalent forms

The class number

Theorem

Let $D \in \mathbb{Z}_{<0}$. There are only finitely many reduced forms of discriminant D.

Proof.

If $Ax^2 + Bxy + Cy^2$ has discriminant $B^2 - 4AC = D$ and is reduced, then as $|B| \leq A \leq C$, we have $-D = 4AC - B^2 \geq 4A^2 - A^2 = 3A^2$, whence $A \leq \sqrt{-D/3}$. Besides, $-A \leq B \leq A$; and finally $C = \frac{B^2-D}{4A}$ is determined by A and B. $\square$

Definition

The class number $h(D)$ is the number of reduced forms of discriminant D.

The class number: example

Example

We determine $h(D)$ for $D = -31$.
Note that as D is odd, B must be odd as well.

We have $A \leq \sqrt{31/3} = 3.2\ldots$.

- $A = 1$:
  - $B = \pm 1 \rightsquigarrow C = \frac{32}{4}$ ✓✗ $\rightsquigarrow x^2 + xy + 8y^2$
- $A = 2$:
  - $B = \pm 1 \rightsquigarrow C = \frac{32}{8}$ ✓✓ $\rightsquigarrow 2x^2 \pm xy + 4y^2$
- $A = 3$:
  - $B = \pm 1 \rightsquigarrow C = \frac{32}{12} \notin \mathbb{Z}$ ✗
  - $B = \pm 3 \rightsquigarrow C = \frac{40}{12} \notin \mathbb{Z}$ ✗

$\rightsquigarrow h(-31) = 3$.

Application: representability when $h = 1$

The class number 1 case

Theorem (Reminder)

Let $D \in \mathbb{Z}$ be 0 or $1 \bmod 4$, and let $n \in \mathbb{Z}$ be odd and coprime to D. Then n is prop. rep. by a primitive form of discriminant $D \iff D$ is a square mod n.

Example

Let $n = 101$, which is prime. As $\left(\frac{-31}{101}\right) = \cdots = +1$, we conclude that 101 is of the form $x^2 + xy + 8y^2$ or of the form $2x^2 \pm xy + 4y^2$, maybe both!

The class number 1 case

Corollary

Let F be a form, and $n \in \mathbb{Z}$ odd and coprime to Δ_F. If $h(\Delta_F) = 1$, then

$$F \text{ properly represents } n \iff \Delta_F \text{ is a square mod } n.$$

Corollary

Let F be a form, and let $p \nmid \Delta_F$ be prime $\neq 2$. If $h(\Delta_F) = 1$,

$$F \text{ represents } p \iff \left(\frac{\Delta_F}{p}\right) = +1.$$

Example

$F(x,y) = x^2 + y^2$ has discriminant $D = -4$, and $h(-4) = 1$.
Thus an odd prime p is represented by $F \iff \left(\frac{-4}{p}\right) = +1$.
Note that $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right)$.

The class number 1 theorem (non examinable)

Theorem (Baker & Heegner & Stark, very difficult)

The only $D \in \mathbb{Z}_{<0}$ *such that* $h(-D) = 1$ *are*

$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$

Remark

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$$