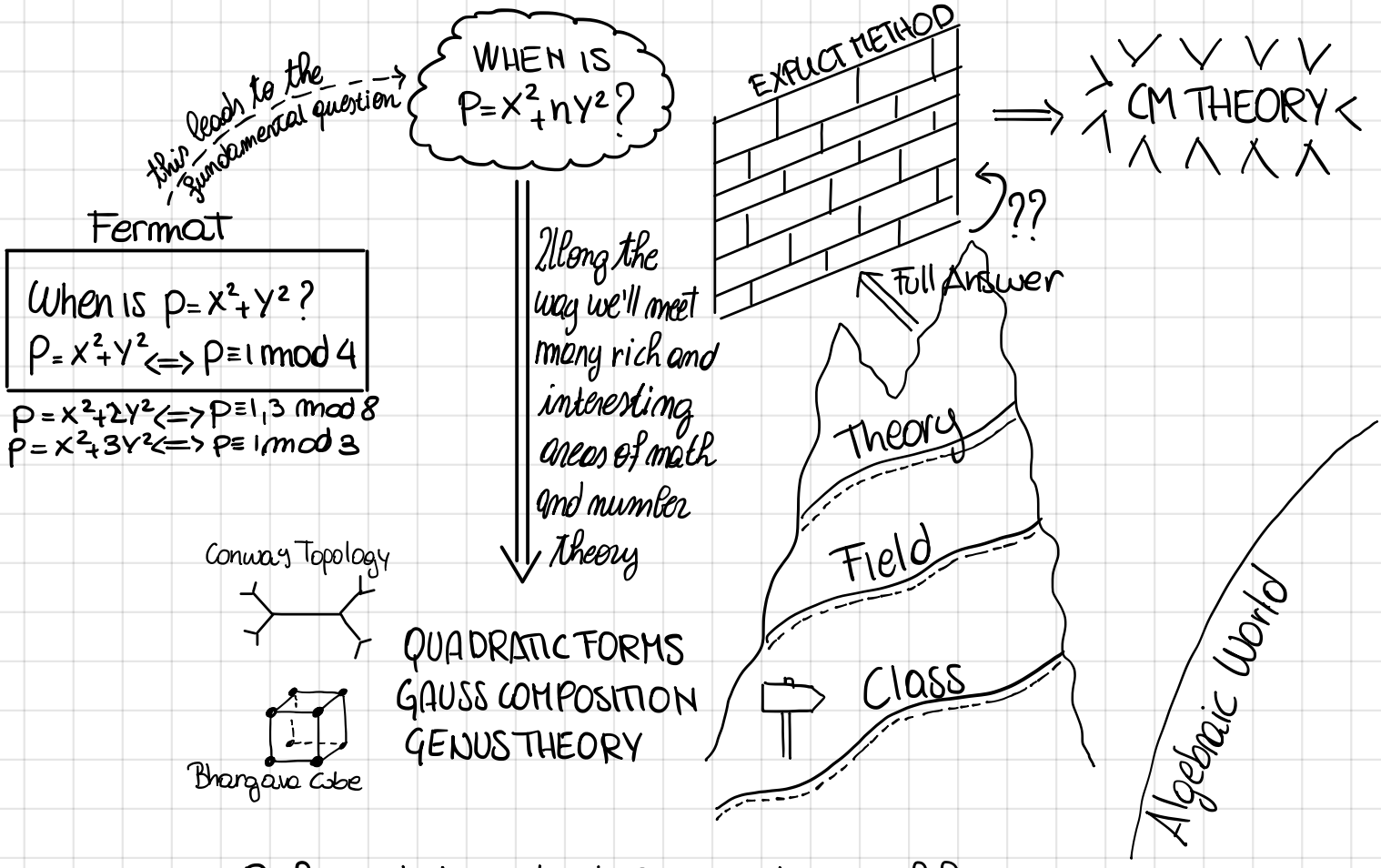
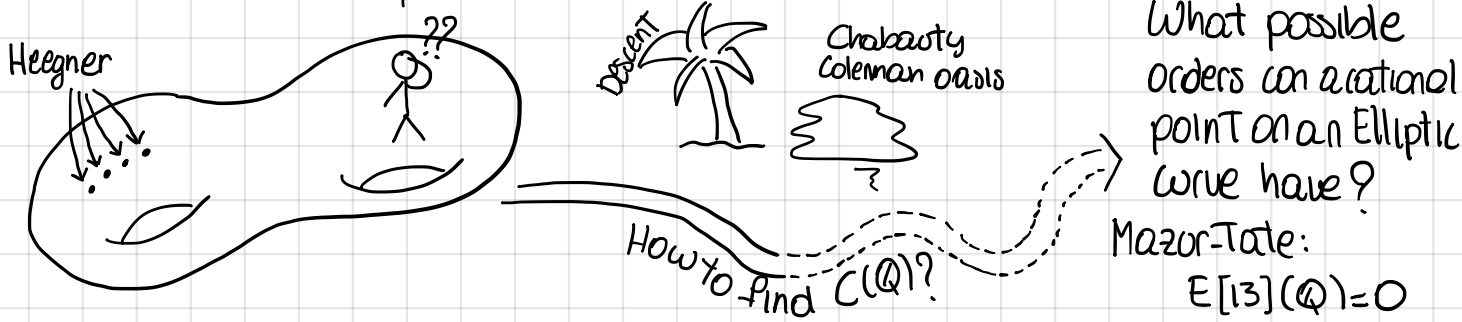


GEOMETRY: Reformulation due to Serre in terms of finding rational points on a non-split Cartan Modular curve.



Picture from "MATH 596: Topics in Algebra and Number Theory", J. Vonk

When is $p=x^2+ny^2$? FIRST WE'LL INVESTIGATE THE PROBLEM USING ELEMENTARY APPROACHES FOLLOWING FERMAT, EULER, LAGRANGE, LEGENDRE AND GAUSS. Around 1640, Fermat conjectured that a prime p can be written as a sum of two squares if and only if it surpasses by one a multiple of 4. He also made similar conjectures: $p=x^2+2y^2 \iff p\equiv 1 \bmod 8$, $p=x^2+3y^2 \iff p\equiv 0,1 \bmod 3$. Once more, he claimed he had a *FIRMISSIMUS DEMONSTRATIONIBUS* but he did not provide any.

It was not until about a century that Euler became interested in these questions and provided full answer. He also gave other conjectures, some similar to Fermat's ones ($p=x^2+5y^2 \iff p\equiv 1,9 \bmod 20$), some quite different

$$p=x^2+27y^2 \iff \begin{cases} p\equiv 1 \bmod 3 \\ 2 \text{ is a cubic residue mod } p \end{cases}$$

A more general approach requires the study of quadratic forms (Lagrange) and a theory of genera. Unfortunately these can solve only part of the problem and this motivated Legendre to develop a theory of composition the relation between all these ideas was exploited by Gauss in his DISQUISITIONES ARITMETICAE (he also proved x^2+27y^2)
GOing Further, requires class field theory which will give us

Theorem $n \equiv 1,2 \bmod 4$ positive square free integer. There exist $f_n(x) \in \mathbb{Z}[x]$ monic and irreducible such that for $p \nmid n$, $p \nmid \operatorname{discr}(f_n)$

$$p = x^2+ny^2 \iff \begin{cases} (-n/p)=1 \\ f_n(x) \equiv 0 \bmod p \text{ has a solution} \end{cases}$$

The main point is to find the polynomials $\Rightarrow$ CFT Theory.

Theorem $p = x^2+y^2 \iff p \equiv 1 \bmod 4$

Proof ($\Rightarrow$) $p = x^2+y^2$, p ODD $\Rightarrow p \equiv 1,3 \bmod 4$. Suppose $p \equiv 3 \bmod 4$
$\Rightarrow 3 \equiv x^2+y^2 \bmod 4$. since p odd, either x or y must be odd
(say x) $\Rightarrow 3 \equiv x^2 \bmod 4$ ↯

($\Leftarrow$) EULER **I. RECIPROCITY** -1 IS A SQUARE MOD $p \iff p \equiv 1 \bmod 4$, i.e., $(-1/p) = (-1)^{\frac{p-1}{2}}$

($\Rightarrow$) $-1 \equiv \alpha^2 \bmod 4 \Rightarrow (-1)^{p-1/2} \equiv \alpha^{p-1} \equiv 1 \bmod p$ (FERMAT'S LITTLE THEOREM)
since p odd $(-1)^{p-1/2} = 1 \Rightarrow \frac{p-1}{2} = 2k \Rightarrow p = 4k+1$

($\Leftarrow$) $p \equiv 1 \bmod 4 \Rightarrow p = 4k+1$
$(x^{4k}-1) = (x^{2k}-1)(x^{2k}+1)$ has $4k$ roots in $\mathbb{F}_p^\times$
(Fermat's little theorem) $\Rightarrow x^{2k}+1$ has $2k$ roots in $\mathbb{F}_p^\times$ ($\mathbb{F}_p$ IS FIELD)
$\Rightarrow -1$ IS A square modulo p

Notice that $p \equiv 1 \bmod 4$ implies $p \mid x^{2k}+1 \Rightarrow p \mid$ sum of two squares

II DESCENT IT is easy (computations) to prove that
$(x^2+y^2)(z^2+w^2) = (xz+yw)^2+(xw-yz)^2$
Now suppose $N = a^2+b^2$, $\gcd(a,b)=1$, $q \mid N$ prime: $q = x^2+y^2$
Then N/q is also sum of 2 squares:
$q \mid (x^2N - a^2q) = x^2a^2+x^2b^2-x^2a^2-y^2a^2 = (xb+ay)(xb-ay)$
without loss of generality (change $a \mapsto -a$) we can assume
$q \mid bx-ay \Rightarrow qd = bx-ay$
$x \mid x(b-dx) = xb-dx^2 = xb-dx^2-dy^2+dy^2 = xb-dq+dy^2$
$= ay+dy^2 = y(a+dy) \Rightarrow xc = a+dy$, $yc = b-dx$ ($(x,y)=1$)

$$\begin{cases} a = xc - dy \\ b = yc + dx \end{cases} \qquad N = a^2+b^2 = (xc-dy)^2 + (yc+dx)^2 = \\ = (x^2+y^2)(c^2+d^2) = q(c^2+d^2)$$

$$\Rightarrow N/q = c^2+d^2$$

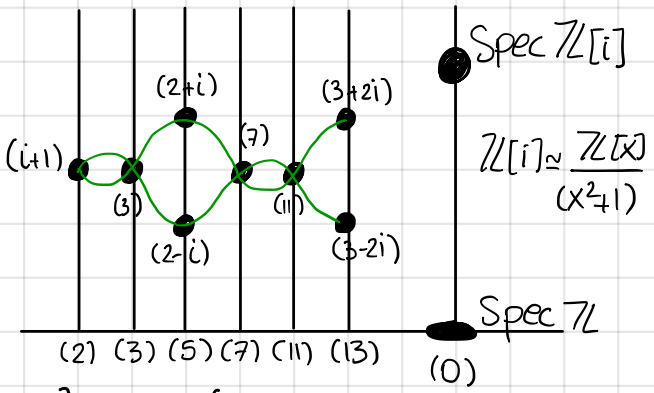
DIVIDING BY p IF NECESSARY

Now, if $p \mid N = a^2+b^2$ then we may assume $2|a|, 2|b| < p$ $\Rightarrow N < p^2/2$. then all $q \mid N$ $q \neq p$ must be less than p. If q is sum of two squares $\Rightarrow N/q > p$ is. IF ALL q ARE $\Rightarrow p$ is sum of 2 SQUARES

($\Longleftarrow$) DEDEKIND

THIS PROOF TAKES PLACES IN $\mathbb{Z}[i]$

KUMMER-DEDEKIND: factorization of (p) in $\mathbb{Z}[i]$ is given by the factorization of x^2+1 in $\mathbb{F}_p[x]$



$p\mathbb{Z}[i]$ has factor $\mathfrak{p} \Longleftrightarrow \mathfrak{p} \supseteq p\mathbb{Z}[i]$

$$\left\{\begin{matrix}\text{Factors of} \\ p\mathbb{Z}[i]\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{Primes of } \mathbb{Z}[i] \\ \text{containing } p\mathbb{Z}[i]\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{\text{primes of } \frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]}\right\}$$

$$\frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]} \simeq \frac{\mathbb{Z}[x]/(x^2+1)}{p\mathbb{Z}[x]+(x^2+1)\mathbb{Z}[x]/(x^2+1)} \simeq \frac{\mathbb{Z}[x]}{p\mathbb{Z}[x]+(x^2+1)\mathbb{Z}[x]} \simeq \frac{\mathbb{Z}[x]/p\mathbb{Z}[x]}{\frac{p\mathbb{Z}[x]+(x^2+1)\mathbb{Z}[x]}{p\mathbb{Z}[x]}} \simeq \frac{\mathbb{F}_p[x]}{(\overline{x^2+1})}$$

$$\left\{\begin{matrix}\text{Monic irreducable} \\ \text{polynomials in } \mathbb{F}_p[x] \\ \text{dividing } (\overline{x^2+1})\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{Primes of } \mathbb{F}_p[x] \\ \text{containing } (\overline{x^2+1})\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{Primes of} \\ \mathbb{F}_p[x]/(\overline{x^2+1})\end{matrix}\right\}$$

-1 IS A SQUARE MODULO $p \Longleftrightarrow p \equiv 1 \bmod 4$

$\Longleftrightarrow (p) = \pi\bar{\pi}$ in $\mathbb{Z}[i]$ which is a P.I.D.

$\pi = (x+iy) \Rightarrow p = x^2+y^2$

($\Longleftarrow$) HEATH-BROWN 1971 ZAGIER

$p = 4m+1$. We define $\mathcal{N} = \{x,y,z \in \mathbb{N} \mid x^2+4yz = p\}$ Finite set

The involution

$$(x,y,z) \longmapsto \begin{cases} (x+2z, z, y-x-z) & x < y-z \\ (2y-x, y, x-y+z) & y-z < x < 2y \\ (x-2y, x-y, y) & 2y < x \end{cases}$$

has one fixed point $(1,1,m)$ - check this with matrices -.

$\Rightarrow \mathcal{N}$ has an odd number of points $\Rightarrow (x,y,z) \to (x,z,y)$ has a fixed point $\Rightarrow p$ is sum of two squares.

As well as proving Fermat's conjecture, Euler raised some other questions like $p = x^2+5y^2 \Longleftrightarrow p \equiv 1, 9 \bmod 30$ but was unable to prove them using descent. Further, for larger n, the criterion gets less and less precise

$$\begin{cases} p = x^2 + 14y^2 \\ p = 2x^2 + 7y^2 \end{cases} \text{ or } \iff p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$$

How to generalize? IN EULER'S PROOF Reciprocity can be generalized

Theorem (AUREM THEOREMA - GAUSS) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ $\left(\frac{2}{p}\right) = (-1)^{p^2-1/8}$

But descent is very specific

DEDEKIND'S PROOF is slightly more general but still relies on some specific cases: for example $\mathbb{Z}[i]$ is a P.I.D. while, in general, $\mathbb{Z}[\sqrt{-n}]$ is not even a Dedekind domain

QUADRATIC FORMS

Definition A binary quadratic form is a homogeneous polynomial of degree 2 in $\mathbb{Z}[X,Y]$ given by $F(x,y) = ax^2 + bxy + cy^2$

Their study began with Lagrange (RESERCHES D'ARITMETIQUE) and was developed by Gauss

Definition
- F IS PRIMITIVE IF $(a,b,c) = 1$ we will only deal with primitive forms.
- $\Delta = b^2 - 4ac$ IS CALLED DISCRIMINANT
  - $\Delta < 0$ DEFINITE $\leftrightarrow$ POSITIVE assume only positive values. / NEGATIVE assume only negative values.
  - $\Delta > 0$ INDEFINITE
  - $\Delta = 0$ PARABOLIC
- An integer n is said to be represented by F if there exist $x, y \in \mathbb{Z}$ such that $F(x,y) = n$. If $(x,y) = 1$ we say PROPERLY REPRESENTED
- $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z}) \mid \alpha\delta - \beta\gamma = \pm 1 \right\}$. we define an action of $SL_2(\mathbb{Z})$ on the set of quadratic forms

$$\Gamma \cdot F(x,y) = F(\alpha x + \beta y, \gamma x + \delta y)$$

we'll usually write $\langle a,b,c \rangle$ for $F(x,y)$ and $\gamma \langle a,b,c \rangle = \langle A,B,C \rangle$

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} \alpha^2 & \alpha\gamma & \gamma^2 \\ 2\alpha\beta & \alpha\delta + \beta\gamma & 2\gamma\delta \\ \beta^2 & \beta\delta & \delta^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

Theorem This action preserves discriminant and primitive forms

Proof $B^2 - 4AC = (2\alpha\beta a + \alpha\delta b + \beta\gamma b + 2\gamma\delta c)^2 - 4(\alpha^2 a + \alpha\gamma b + \gamma^2 c)(\beta^2 a + \beta\delta b + \delta^2 c) =$

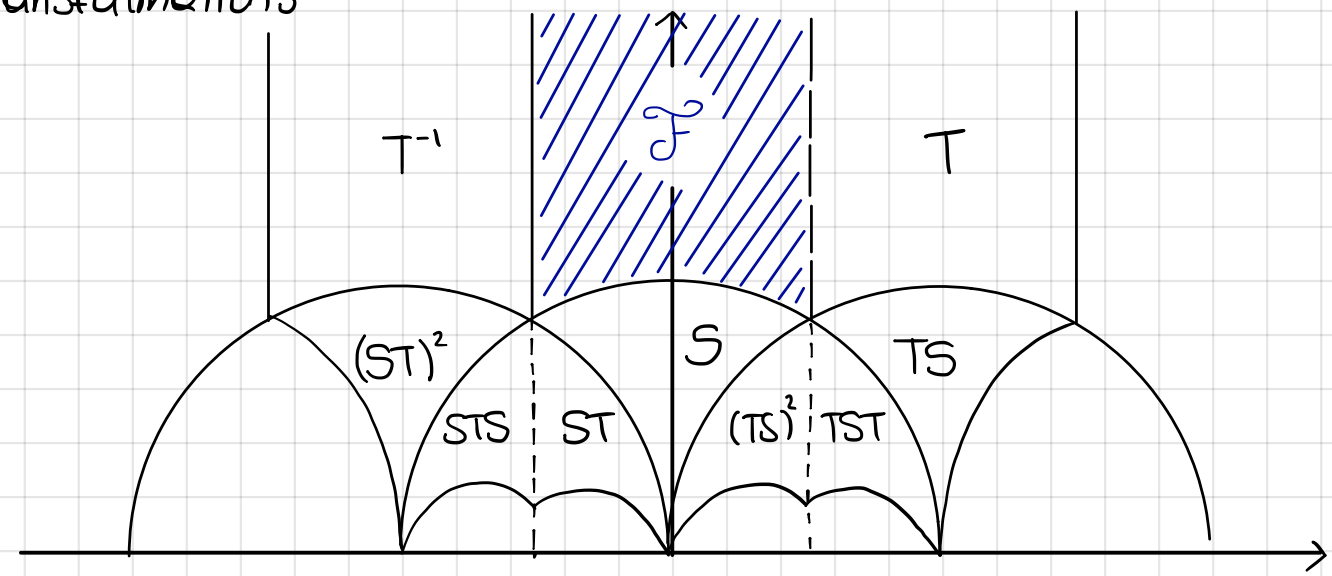
$= 4\alpha^2\beta^2 a^2 + \alpha^2\delta^2 b^2 + 4\alpha^2\beta\delta ab + \beta^2\gamma^2 b^2 + 4\gamma^2\delta^2 c^2 + 4\beta\gamma^2\delta bc + 4\alpha\beta^2\gamma ab + 8\alpha\beta\gamma\delta ac$
$+ 2\alpha\beta\gamma\delta b^2 + 4\alpha\gamma\delta^2 bc - 4\alpha^2\beta^2 a^2 - 4\alpha^2\beta\delta ab - 4\alpha^2\delta^2 ac - 4\alpha\beta\gamma\delta b^2 - 4\alpha\beta^2\gamma ab - 4\alpha\gamma\delta^2 bc$
$- 4\beta^2\gamma^2 ac - 4\beta\gamma^2\delta bc - 4\gamma^2\delta^2 c^2 = \alpha^2\delta^2 b^2 - 2\alpha\beta\gamma\delta b^2 - 4\alpha^2\delta^2 ac - 4\beta^2\gamma^2 ac + 8\alpha\beta\gamma\delta ac$
$+ \beta^2\gamma^2 b^2 = b^2(\alpha\delta - \beta\gamma)^2 - 4ac(\alpha\delta - \beta\gamma)^2 = (b^2 - 4ac)(\alpha\delta - \beta\gamma)^2 = \Delta(\det\Gamma)^2 = \Delta = b^2 - 4ac$

DEFINITE QUADRATIC FORMS

Every orbit consist of all positive or all negative definite quadratic forms $\langle a,b,c\rangle \longrightarrow \langle -a,b,-c\rangle$ interchanges the two $\Rightarrow$ there is no essential difference between the two theories.

Definition A POSITIVE DEFINITE QUADRATIC FORM $\langle a,b,c\rangle$ IS REDUCED IF $|b|\le a\le c$ AND $b\ge 0$ IF EITHER $|b|=a$ OR $a=c$
A NEGATIVE DEFINITE FORM IS REDUCED IF THE CORRESPONDING POSITIVE DEFINITE FORM IS

This definition has a more visual interpretation as it is equivalent to say That one of the roots of ax^2+bx+c lies in the standard fundamental domain of $SL_2(\mathbb{Z})$ in its action on the upper half plane $\mathcal{H}$ via linear fractional transformations



$\tau = p+iq \quad a(p+iq)^2+b(p+iq)+c=0 \quad ap^2+bp-aq^2+c+i(2apq+bq)=0$

$$\begin{cases} 2apq+bq=0 \\ ap^2+bp-aq^2+c=0 \end{cases} \Rightarrow q(2ap+b)=0 \quad 2ap+b=0 \quad p=-\frac{b}{2a} \text{ IF REDUCED}$$

$\text{Re}(\tau)$ $\qquad p\in[-\frac{1}{2},\frac{1}{2})$

$$0=\frac{b^2}{4a}-\frac{b^2}{2a}-aq^2+c=-\frac{b^2}{4a}-aq^2+c \Rightarrow q^2=\frac{c}{a}-\frac{b^2}{4a^2} \qquad |\tau|=\sqrt{\frac{b^2+4ac-b^2}{4a^2}}=\sqrt{\frac{c}{a}}$$

IF F reduced $|\tau|\ge 1$

Theorem EVERY DEFINITE FORM IS EQUIVALENT TO ONE AND ONLY ONE REDUCED FORM

Proof Easy from the properties of fundamental domain

An immediate consequence of this is that the number of equivalence classes of primitive forms of given discriminant is finite. Indeed, for a reduced form we have $b^2 \le a^2$, $a \le c \Rightarrow \Delta = b^2 - 4ac \le a^2 - 4a^2 = -3a^2$ $\Rightarrow$ finitely many possibilities for $a \Rightarrow$ hence for $b \Rightarrow$ hence for c.

Definition The number of reduced primitive forms of discriminant Δ is said CLASS NUMBER: $h^+(\Delta)$

Δ		Δ		Δ		Δ	
-3	$\langle 1,1,1\rangle$	-16	$\langle 1,0,4\rangle$	-31	$\langle 1,1,8\rangle, \langle 2,\pm 1,4\rangle$	-256	$\langle 1,0,64\rangle$
-4	$\langle 1,0,1\rangle$	-19	$\langle 1,1,5\rangle$	-32	$\langle 1,0,8\rangle, \langle 3,2,3\rangle$		$\langle 4,4,17\rangle$
-7	$\langle 1,1,2\rangle$	-20	$\langle 1,0,5\rangle, \langle 2,2,3\rangle$	-56	$\langle 1,0,14\rangle$		$\langle 5,\pm 2,13\rangle$
-8	$\langle 1,0,2\rangle$	-23	$\langle 1,1,6\rangle, \langle 2,\pm 1,3\rangle$		$\langle 2,0,7\rangle$	-512	$\langle 1,0,128\rangle$
-11	$\langle 1,1,3\rangle$	-24	$\langle 1,0,6\rangle, \langle 2,0,3\rangle$		$\langle 3,\pm 2,5\rangle$		$\langle 3,\pm 2,43\rangle$
-12	$\langle 1,0,3\rangle$	-27	$\langle 1,1,7\rangle$	-108	$\langle 1,0,27\rangle$		$\langle 4,4,33\rangle$
-15	$\langle 1,1,4\rangle, \langle 2,1,2\rangle$	-28	$\langle 1,0,7\rangle$		$\langle 4,\pm 2,7\rangle$		$\langle 9,\pm 8,16\rangle$
							$\langle 11,\pm 4,12\rangle$

If one continues this table, one might conjecture that $h^+(\Delta)$ grows as $C\sqrt{-\Delta}$: 1930 DEURING, HILBRONN, SIEGEL $\forall \varepsilon > 0$ $h^+(\Delta) \ge C_\varepsilon |\Delta|^{1/2-\varepsilon}$

1976 GOLDFELD: $\exists$ elliptic curve E : $\mathcal{L}_E$ vanishes at $s=1$ to order 3 implying that $h^+(\Delta) \ge C_\varepsilon \log |\Delta|$

1983 GROSS-ZAGIER, They found E and OSTERLÉ determined $C_\varepsilon = \frac{1}{7000}$

INDEFINITE QUADRATIC FORMS

The Theory for indefinite forms is significantly richer and more mysterious than its counterpart. It does not exist a notion of reduced form assuring all the nice properties above. We'll assume Δ nonsquare (NONDEGENERATE CASE)

$F = \langle a,b,c\rangle$ $\Delta > 0$ IS REDUCED IF $0 < \sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b$ WHICH IS EQUIVALENT TO THE FOLLOWING CONDITIONS ON ROOTS

$$\begin{cases} \lambda^+ \ge 1 \text{ AND } \lambda^- \in (-1,0) & \text{IF } a \ge 0 \\ \lambda^- \le -1 \text{ AND } \lambda^+ \in (0,1) & \text{IF } a \le 0 \end{cases}$$

Note that in this case there might be more than one reduced form per orbit

eg $\Delta = 2021$ $\langle 5,41,-17\rangle$, $\langle 19,11,-25\rangle$ $T = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$

Definition $F = \langle a,b,c\rangle$ ITS RIGHT NEIGHBOUR $\rho(F) = \langle c, -b + 2sc, cs^2 - bs + a\rangle$

$$s = \begin{cases} \operatorname{sgn}(c) \left\lfloor \frac{b}{2|c|} \right\rfloor & |c| > \sqrt{\Delta} \\ \operatorname{sgn}(c) \left\lfloor \frac{b+\sqrt{\Delta}}{2|c|} \right\rfloor & |c| < \sqrt{\Delta} \end{cases}$$

Every indefinite form is equivalent to a reduced form

- IF F IF REDUCED $\Rightarrow \rho(F)$ IS REDUCED TO
- $\Delta_{\rho(F)} = b^2 + 4\cancel{a^2c^2} - 4\cancel{b}ac - 4\cancel{a^2}c^2 + 4\cancel{b}ac - 4ac = b^2 - 4ac = \Delta_F$
- SUPPOSE $|a| > \sqrt{\Delta} \Rightarrow |c| < |a|$ $b^2 > 0$ AND THE SIZE OF THE FIRST COEFFICIENT OF $\rho(F)$ IS STRICTLY LESS THAN THE ONE OF F

By replacing F by $\rho(F)$ we may assume $|a| < \sqrt{\Delta} \Rightarrow \rho(F)$ IS reduced $\Rightarrow$ Hence, at a certain point we hit a reduced form.

Remark SINCE THERE ARE FINITELY MANY REDUCED FORMS, THE SEQUENCE $F, \rho(F), \rho^2(F), \dots, \rho^i(F), \dots$ IS EVENTUALLY PERIODIC

eg $F = \langle 1, 0, -67 \rangle$ $\Delta = 268$ $\rho(F) = \langle -67, 0, 1 \rangle$ $\rho^2(F) = \langle 1, 16, -3 \rangle$

not reduced REDUCED

$1^{\overset{b_F}{0}} \; -67^{\overset{b_{\rho(F)}}{0}} \; 1^{16} \; -3^{14} \; 6^{10} \; -7^{4} \; 9^{14} \; -2^{14} \; 9^{4} \; -7^{10} \; 6^{14} \; -3^{16} \; 1^{16}$

a_F $a_{\rho(F)}$

are reduced Periodicity = 10

Two reduced forms (indefinite) are equivalent $\Leftrightarrow$ they live in the same cycle

Remark WE WON'T NEED IT BUT NOTICE THAT THERE IS AN INTIMATE CONNECTION WITH CONTINUED FRACTIONS

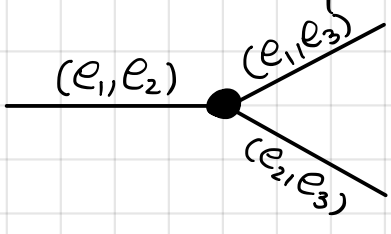
PARABOLIC FORMS

This case is not deep or rich in applications. Reduced if $a = b = 0$

Theorem ANY PARABOLIC FORM IS EQUIVALENT TO A UNIQUE REDUCED FORM

CONWAY'S TOPOLOGY

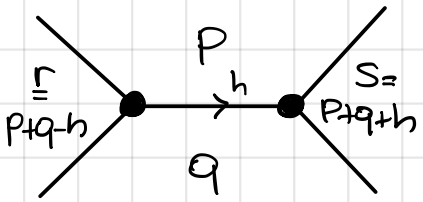
CONWAY PRESENTS A NICE AND INTUITIVE WAY OF INVESTIGATING QUADRATIC FORMS. We know that $SL_2(\mathbb{Z}) \simeq C_4 *_{C_2} C_6$ AND THIS CORRESPONDS TO AN ACTION OF $SL_2(\mathbb{Z})$ ON A TREE WHICH IS 3-REGULAR EDGES = Basis of a $\mathbb{Z}$-lattice of dimension 2 up to sign. Two edges shares a vertex if they share one of the two vectors of the basis up to sign



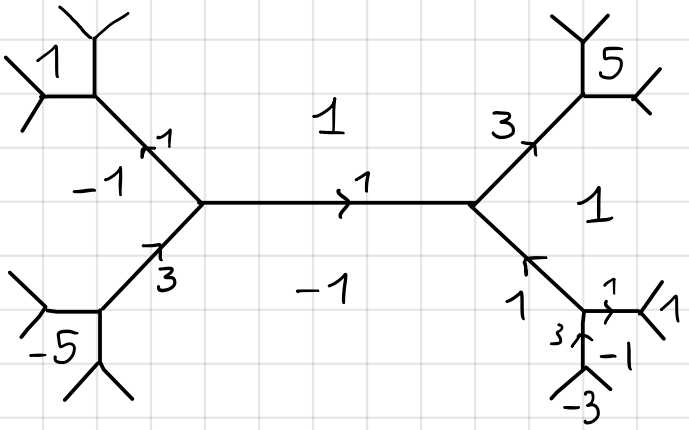
We may embed this in the plane so that two edges sharing one vertex are adjacent to the same region of the plane.

$\Rightarrow$ the resulting object is called TOPOGRAPH.

The convention is that the value assigned to an edge is always positive and the region to the left is the first vector of the basis. The value of the edge between p and s is the positive square root of $\Delta + 4pq$ and it is pointing towards q if $q > p+s$ and away otherwise

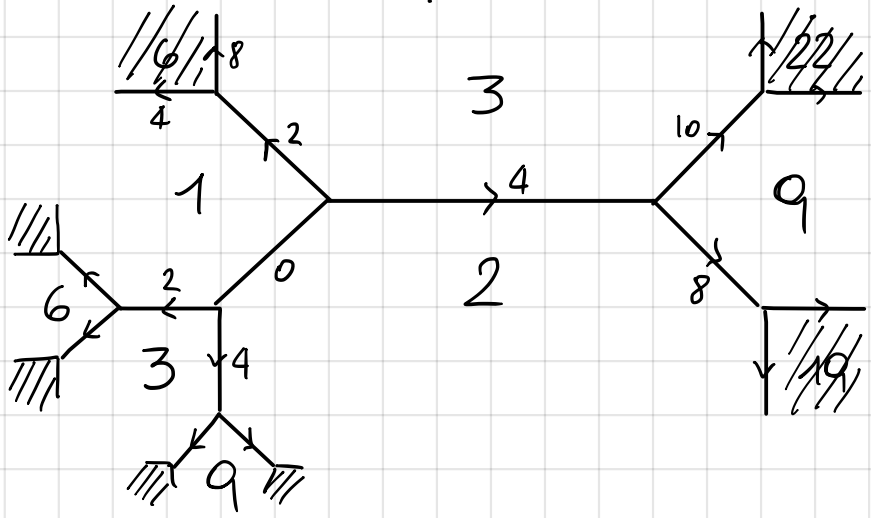


eg $\langle 1,1,-1\rangle$ $\Delta = 5$



Lemma (Climbing Lemma) IF $p,q>0$ THEN $S>0$ AND ALL EDGES ADJACENT TO S POINT AWAY FROM THE VERTEX (p,q,s)

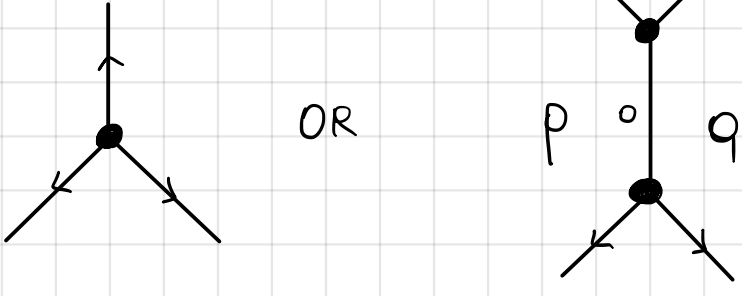
eg Is $5 = 3X^2 + 4XY + 2Y^2$? $F = \langle 3,4,2\rangle$ $\Delta = -8$



NO!

DEFINITE FORMS

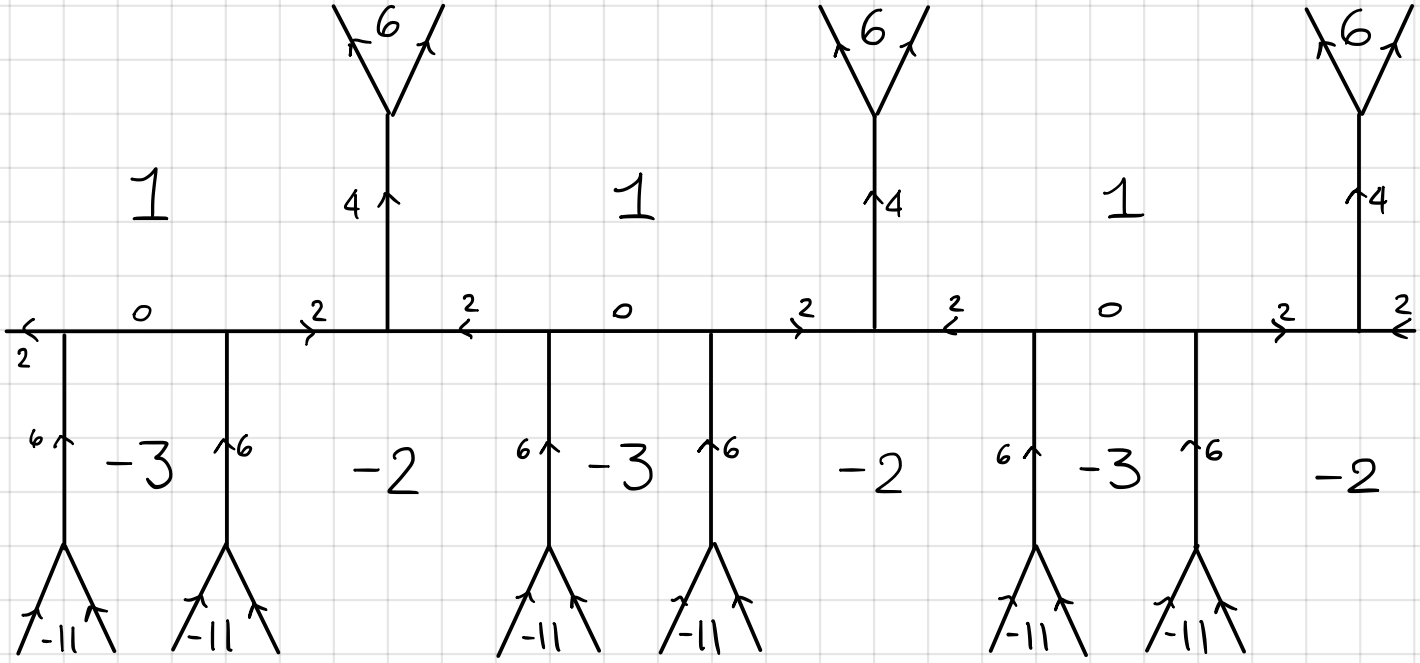
There is no essential difference between positive and negative definite forms. By climbing lemma, if we follow the flow of the arrows then the values of all regions keep increasing. Then there must be a "source":



INDEFINITE FORMS

$\Delta > 0$ NON-SQUARE. THEN F REPRESENTS BOTH POSITIVE AND NEGATIVE VALUES BUT NOT 0. THEN THERE MUST BE AN EDGE ADJACENT TO REGIONS OF OPPOSITE SIGN. Following the procedure to complete the topograph starting from this edge we see that either side of this edge there must be another edge with the same property. THE EDGING SEPARATING POSITIVE AND NEGATIVE VALUES MUST BE AN INFINITE CHAIN (RIVER)

$\Delta = 12$ $\langle 1, 0, 3 \rangle$

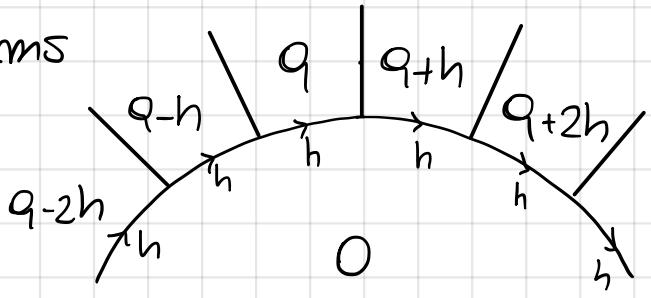


By climbing lemma, moving away from the river, absolute values increase.

Remark The river is the most interesting part. Note that the condition $pq<0$ means that $h^2 - 4pq > 0$ has only finitely many possibilities and hence the river must eventually become periodic

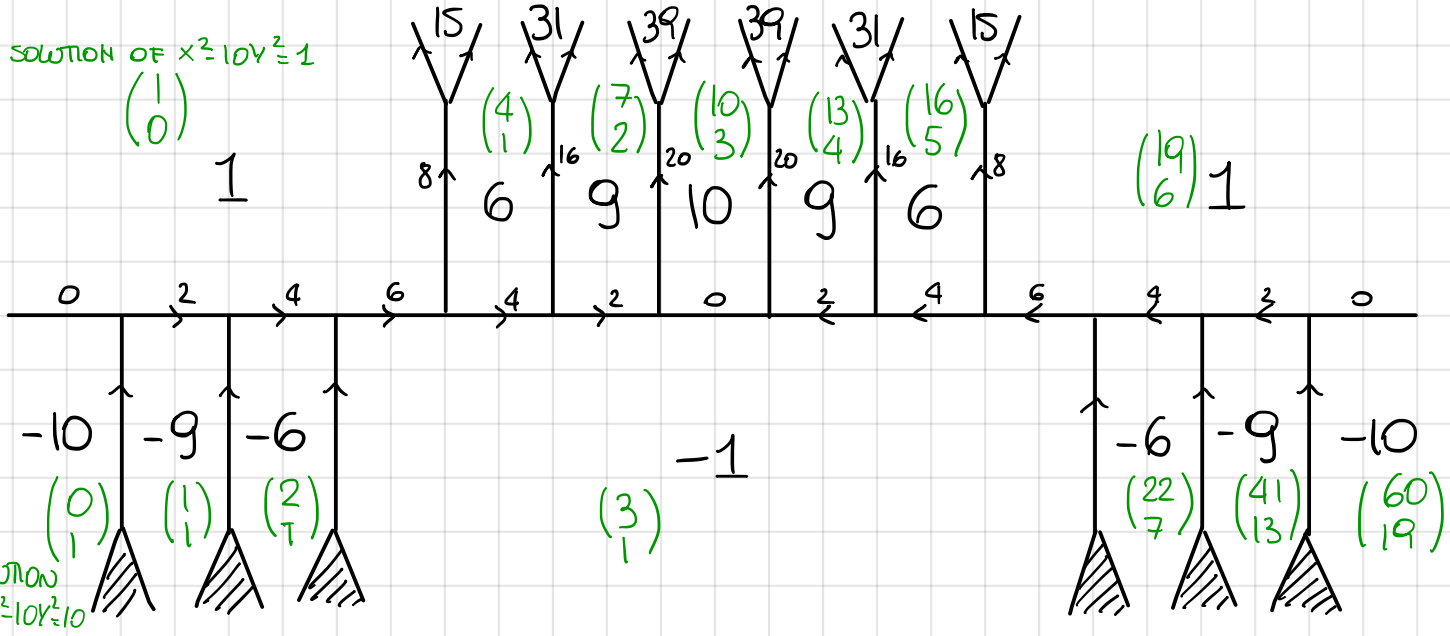
Remark Do you recall the Conway definition of reduced form? This corresponds to an edge of the river where the trees hanging from the river switches from region + to region − or vice versa.

In the example we get two reduced forms $\langle 1, 2, -2 \rangle$ and $\langle 1, -2, -2 \rangle$



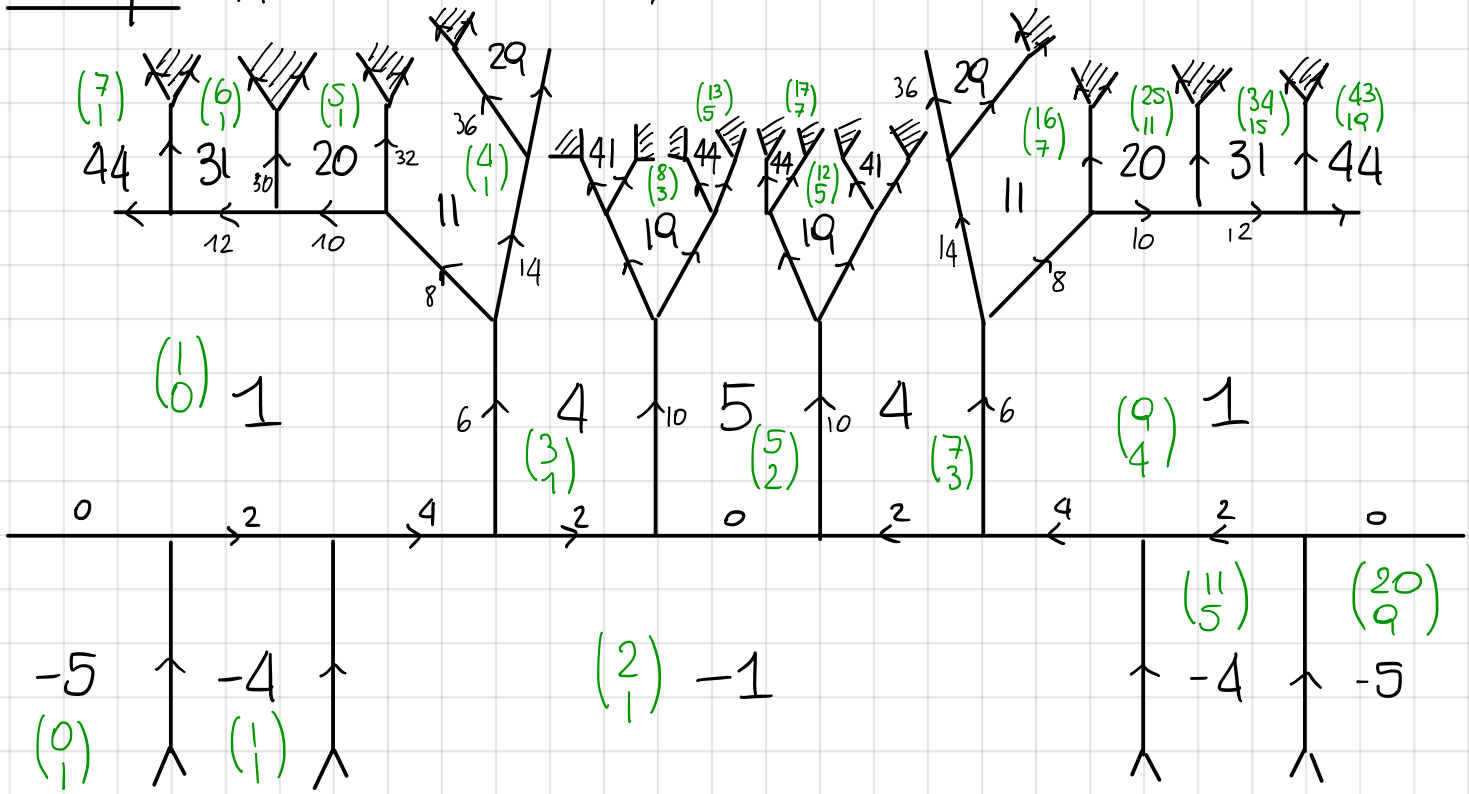
IF $\Delta = h^2$ The form has rational root $\Rightarrow$ IT REPRESENTS 0 $\Rightarrow$ THERE IS A REGION LABELED 0 (LAKE)

example is $9 = x^2 - 10y^2$? $\Delta = 40$



$$\text{SOLUTIONS} = \left\{ \pm T^{\mathbb{Z}} \begin{pmatrix}3\\0\end{pmatrix}, \pm T^{\mathbb{Z}} \begin{pmatrix}7\\2\end{pmatrix}; \pm T^{\mathbb{Z}} \begin{pmatrix}13\\4\end{pmatrix} \right\} \quad T = \begin{pmatrix}19 & 60\\6 & 19\end{pmatrix}$$

example $44 = x^2 - 5y^2$? $\langle 1, 0, -5 \rangle$ $\Delta = 20$



$$\text{SOLUTIONS} = \left\{ \pm T^{\mathbb{Z}} \begin{pmatrix}7\\1\end{pmatrix}; \pm T^{\mathbb{Z}} \begin{pmatrix}8\\2\end{pmatrix}; \pm T^{\mathbb{Z}} \begin{pmatrix}13\\5\end{pmatrix}; \pm T^{\mathbb{Z}} \begin{pmatrix}17\\7\end{pmatrix}; \pm T^{\mathbb{Z}} \begin{pmatrix}32\\14\end{pmatrix}; \pm T^{\mathbb{Z}} \begin{pmatrix}43\\19\end{pmatrix} \right\} \quad T = \begin{pmatrix}9 & 20\\4 & 9\end{pmatrix}$$

IF THE ARROW POINTS IN THE RIGHT DIRECTION WE TAKE AS FIRST VECTOR THE ONE ON THE LEFT, OTHERWISE WE SWAP THE ARROW (OPPOSITE DIRECTION) AND TAKE AGAIN THE ONE ON THE LEFT. IF $\det \begin{pmatrix}v_1 & w_1\\v_2 & w_2\end{pmatrix} > 0 \Rightarrow \text{sum } \begin{pmatrix}v_1\\v_2\end{pmatrix} + \begin{pmatrix}w_1\\w_2\end{pmatrix}$
IF $\det < 0$ WE CHANGE THE SIGN TO THE FIRST VECTOR (OR SECOND - BUT ONCE CHOOSEN I CANNOT CHANGE) AND SUM
($\uparrow$ I VECTOR, $\uparrow$ II VECTOR)

GAUSS COMPOSITION

Now that we have a good understanding of the action of $SL_2(\mathbb{Z})$, we introduce a new tool: COMPOSITION LAW. For Gauss, the existence of a composition law (NATURAL GROUP LAW) on classes was one of the reasons to consider $SL_2(\mathbb{Z})$-orbits rather than $GL_2(\mathbb{Z})$-orbits.

Definition $H(x,y)$ IS DIRECT COMPOSITION OF TWO QUADRATIC FORMS $F(x,y)$ AND $G(x,y)$ IF THERE ARE TWO BILINEAR FORMS

$$B_1(x,y,z,w) = a_1xz + b_1xw + c_1yz + d_1yw$$
$$B_2(x,y,z,w) = a_2xz + b_2xw + c_2yz + d_2yw$$

SUCH THAT $F(x,y)\cdot G(z,w) = H(B_1,B_2)$ AND

$$\begin{cases} a_1b_2 - a_2b_1 = F(1,0) \\ a_1c_2 - a_2c_1 = G(1,0) \end{cases}$$

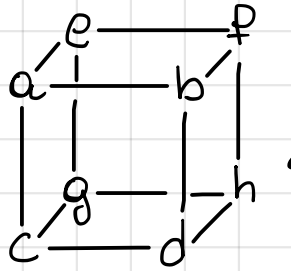
this is added in order to restrict the number of possibilities and have a well defined group-action.

Clearly this notion formalizes the identity that was of crucial importance in the descent step in Euler's proof. GAUSS WENT ON SHOWING THAT IT ENDOW THE SET OF EQUIVALENCE CLASSES OF QUADRATIC FORMS WITH THE STRUCTURE OF FINITE ABELIAN GROUP.

Lemma IF Q_1, Q_2 ARE QUADRATIC FORMS REPRESENTING m AND n RESPECTIVELY AND Q_3 IS DIRECT COMPOSITION OF Q_1 AND $Q_2 \Rightarrow Q_3$ REPRESENTS $m\cdot n$

IN 2004 BHARGAVA PRESENTED A NEW TREATMENT FOR GAUSS COMPOSITION.

Definition WE DEFINE A BHARGAVA CUBE TO BE A 2x2x2 CUBE WITH INTEGERS ASSOCIATED TO ITS VERTICES



we associate to it 3 quadratic forms

$$Q_1(x,y) = -\det\left[\begin{pmatrix} a & e \\ b & f \end{pmatrix}x + \begin{pmatrix} c & g \\ d & h \end{pmatrix}y\right]$$
$$Q_2(x,y) = -\det\left[\begin{pmatrix} a & c \\ e & g \end{pmatrix}x + \begin{pmatrix} b & d \\ f & h \end{pmatrix}y\right]$$
$$Q_3(x,y) = -\det\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}x + \begin{pmatrix} e & f \\ g & h \end{pmatrix}y\right]$$

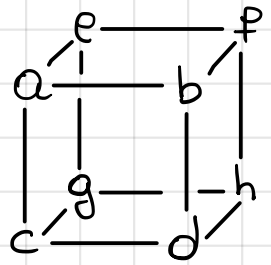
Remark THEY HAVE THE SAME DISCRIMINANT

$$\Delta = a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 + 4adfg + 4bceh - 2abgh - 2acfh - 2adeh - 2bcfg - 2bdeg - 2cdef$$

Remark IF Q_1 AND Q_2 ARE PRIMITIVE, SO IT IS Q_3 (PROJECTIVE CUBE)

Remark $Q_3(X,-Y)$ IS DIRECT COMPOSITION OF Q_1 AND Q_2

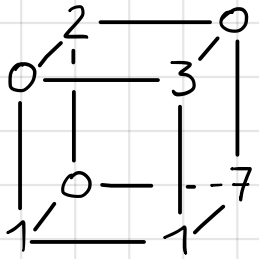
example $\langle 6,2,7\rangle \quad \Delta = -164$
$\langle 2,2,21\rangle$



$$Q_1(X,Y) = 6X^2+2XY+7Y^2 = -\det\begin{pmatrix} aX+cY & eX+gY \\ bX+dY & fX+hY \end{pmatrix}$$
$$= bex^2+dex+bgxy+dgy^2-afx^2-ahxy-cfxy-chy^2 =$$
$$= x^2(be-ah)+xy(de+bg-ah-cf)+y^2(dg-ch)$$

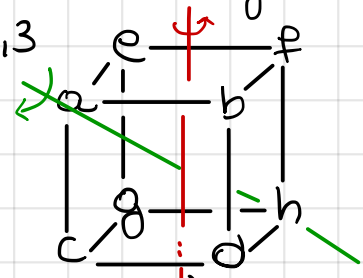
$$Q_2(X,Y) = 2X^2+2XY+21Y^2 = -\det\begin{pmatrix} aX+bY & cX+dY \\ eX+fY & gX+hY \end{pmatrix} =$$
$$= cex^2+cfxy+dexy+df y^2-agx^2-ahxy-bgxy-bhy^2 =$$
$$= x^2(ce-ag)+xy(de+cf-bg-ah)+y^2(df-bh)$$

$$\begin{cases} be-ah=6 \\ de+bg-ah-cf=2 \\ dg-ch=7 \\ ce-ag=2 \\ de+cf-bg-ah=2 \\ df-bh=21 \\ \Delta=-164 \end{cases} \quad \Big\} \; bg+cf=c \qquad \begin{cases} \Delta=-164 \\ be=6 \\ de-ah=2 \\ ch=-7 \\ ec=2 \\ bh=-21 \\ f=g=0 \end{cases} \qquad \begin{cases} a=0 \\ b=3 \\ c=1 \\ d=1 \\ e=2 \\ f=g=0 \\ h=-7 \end{cases}$$



$$Q_3(X,Y) = -\det\begin{pmatrix} 2Y & 3X \\ X & X-7Y \end{pmatrix} = 3X^2-2XY+14Y^2 = \langle 3,-2,14\rangle$$
$$\Rightarrow Q_1Q_2 = \langle 3,2,14\rangle$$

Remark Symmetry group of a cube has order 48. IF $\mathcal{U}$ is a Bhargave cube giving rise to $Q_i = \langle A_i, B_i, C_i\rangle \quad i=1,2,3$



→ ROTATION ABOUT $\overline{ah}$ BY $2\pi/3$
$$(Q_1,Q_2,Q_3) \xrightarrow{\vartheta_1} (Q_3,Q_1,Q_2)$$
→ ROTATION ABOUT A VERTICAL AXIS BY $\pi/2$
$$(Q_1,Q_2,Q_3) \xrightarrow{\vartheta_2} (\langle -A_1,-B_1,-C_1\rangle, \langle C_3,B_3,A_3\rangle, \langle -A_2,-B_2,-C_2\rangle)$$
→ REFLECTION FRONT BACK
$$(Q_1,Q_2,Q_3) \xrightarrow{\vartheta_3} (\langle -A_1,-B_1,-C_1\rangle, \langle -A_2,-B_2,-C_2\rangle, \langle C_3,B_3,A_3\rangle)$$

Observe that $\vartheta_3\circ\vartheta_2\circ\vartheta_1 : (Q_1,Q_2,Q_3) \mapsto (Q_2,Q_1,Q_3)$

Remark IT IS ALSO POSSIBLE TO DEFINE AN ACTION OF $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ ON THE SET OF BHARGAVA CUBES

Definition WE SAY THAT THREE PRIMITIVE QUADRATIC FORMS Q_1, Q_2, Q_3 ARE COLLINEAR IF THERE IS A PROJECTIVE BHARGAVA CUBE WITH PRECISELY THESE THREE FORMS ASSOCIATED

Theorem GIVEN TWO PRIMITIVE FORMS Q_1, Q_2 WITH THE SAME DISCRIMINANT Δ, THERE IS ALWAYS A FORM Q_3 WITH DISCRIMINANT Δ SUCH THAT Q_1, Q_2, Q_3 ARE COLLINEAR, AND ANY TWO SUCH FORMS ARE EQUIVALENT. DECLARING COLLINEAR TRIPLES TO HAVE PRODUCT 1 (OR 0) MAKES THE SET OF EQUIVALENCE CLASSES OF PRIMITIVE FORMS OF DISCRIMINANT Δ INTO A FINITE ABELIAN GROUP.

$$\underset{\text{Principal form}}{\text{IDENTITY}} \quad \left\langle 1, \sigma, \frac{\sigma^2-\Delta}{4} \right\rangle \quad \sigma \in \{0,1\} \quad \sigma^2 \equiv \Delta \bmod 4$$

INVERSE OF $\langle a,b,c \rangle$ IS $\langle a,-b,c \rangle$

WE WRITE $Cl^+(\Delta)$ = EQUIVALENCE CLASSES OF QUADRATIC FORMS OF DISCRIMINANT Δ

We will see the connection with the class number of number fields.

First we define an action of $GL_2(\mathbb{Z})$ $\quad T = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z})$

$$T \cdot F(x,y) = \frac{1}{\det T} F(px+qy, rx+sy)$$

$Cl(\Delta) = GL_2(\mathbb{Z})$-orbits. we have a natural map $\pi: Cl^+(\Delta) \longrightarrow Cl(\Delta)$
we know $[GL_2(\mathbb{Z}) : SL_2(\mathbb{Z})] = 2$ Thus, the fibers of π have order at most 2
LET $[Q_1], [Q_2] \in Cl(\Delta) \Rightarrow [Q_1]\cdot[Q_2] = \pi(\pi^{-1}(Q_1)\cdot\pi^{-1}(Q_2))$

$$1 \longrightarrow \{\pm 1\}/Nm \longrightarrow Cl^+(\Delta) \longrightarrow Cl(\Delta) \longrightarrow 1$$

$Nm = \{\pm 1\}$ if the principal form represents -1 and trivial otherwise.

GENUS THEORY

Now we return to our initial question on how to generalize Fermat's conjecture

Question Which values in $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ are represented by a form of discriminant Δ?

Lemma ALL ELEMENTS IN $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ THAT ARE REPRESENTED BY THE PRINCIPAL FORM, FORM A SUBGROUP H. IF F IS ANY QUADRATIC FORM OF DISCRIMINANT Δ, THEN ALL ELEMENTS IN $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ REPRESENTED BY F FORM A COSET OF H

Proof IT IS A CONSEQUENCE OF GAUSS COMPOSITION

- Observe that principal forms always represents 1 and Gauss composition shows that H is closed under products - $Q_P Q_P = Q_P$
  Further, if a is represented by Q_P, then a^n is as well proving that H contains inverses
- Gauss composition shows that if $a \in (\mathbb{Z}/\Delta\mathbb{Z})^\times$ is represented by F and t is the order of F in $Cl^+(\Delta)$, then $a^t = h \in H$ and $a^{-1}h$ is represented by F^{-1}. IT follows that if a, b are represented by F then $a^{-1}b \in H$. Further, any quadratic form represents values coprime to Δ so the set of values represented by F is non empty $\Rightarrow$ coset of H
  Here we are using Lemma 2.25 of Cox's book.

Definition TWO QUADRATIC FORMS ARE IN THE SAME GENUS IF THEY REPRESENT THE SAME VALUES IN $(\mathbb{Z}/\Delta\mathbb{Z})^\times$. *Clearly, equivalent quadratic forms are in the same genus but, in general, genera consist of several classes.*

$$\Phi : Cl^+(\Delta) \xrightarrow[\text{homomorphisms}]{\text{group}} (\mathbb{Z}/\Delta\mathbb{Z})^\times / H$$

LET r BE THE NUMBER OF ODD PRIMES DIVIDING Δ. WE DEFINE $\mu = \begin{cases} r & \Delta \equiv 1 \bmod 4 \\ r+1 & \text{otherwise} \\ r+2 & h \equiv 0 \bmod 8 \end{cases}$ where $\Delta = -4n$

WE ALSO DEFINE THE CHARACTERS

$$\Delta = \prod_{i=1}^{r} p_i^{e_i} \qquad \chi_i = \left(\frac{\cdot}{p_i}\right) \qquad \delta := (-1)^{(\cdot - 1)/2} \qquad \zeta := (-1)^{(\cdot^2 - 1)/8}$$

THUS, WE GET $\Psi : (\mathbb{Z}/\Delta\mathbb{Z})^\times \longrightarrow \{\pm 1\}^\mu$ AND $\ker \Psi = \bigcap_{i=1}^{n} \ker \chi_i \cap \ker \delta \cap \ker \zeta$

Theorem $\ker \Psi = H$

Proof We'll only prove the case where Δ is odd - we'll only consider χ_i's ELEMENTS MAPPED TO ONE ARE SQUARES IN $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ *chinese remainder Theo.* On the other hand, squares in $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ are represented by principal form $4\left(x^2 + xy + \frac{1-\Delta}{4} y^2\right) \equiv (2x+y)^2 \bmod \Delta$

THIS TELLS US THAT H HAS INDEX AT MOST 2^μ IN $(\mathbb{Z}/\Delta\mathbb{Z})^\times$

Theorem THERE IS A UNIQUE HOMOMORPHISM $\chi: (\mathbb{Z}/\Delta\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ SUCH THAT FOR $p \nmid 2\Delta$, $\chi(p) = \left(\frac{\Delta}{p}\right)$ AND $\chi(-1) = \begin{cases} 1 & \text{IF } \Delta > 0 \\ -1 & \text{IF } \Delta < 0 \end{cases}$

ANY PRIME $p \nmid 2\Delta$ IS REPRESENTED BY SOME FORM OF DISCRIMINANT Δ IF AND ONLY IF $p \in \ker \chi$

Proof The existence of χ is deduced by repeatedly applying Quadratic reciprocity. In fact, the existence of χ is equivalent to quadratic reciprocity. For the second statement note that any form F that properly represents p is equivalent to $\langle p, b, c\rangle$ => if p is represented by some form of discriminant Δ, then $\Delta = b^2 - 4pc \equiv b^2 \bmod p$
$\Rightarrow \left(\frac{\Delta}{p}\right) = 1 \Rightarrow \chi(p) = 1 \Rightarrow p \in \ker \chi$
Vice versa, if $\Delta \equiv b^2 \bmod p$, then we may assume $b \equiv \Delta \bmod 2$
$\Rightarrow \Delta - b^2 \equiv -4c$ some $c \Rightarrow \langle p, b, c\rangle$ has discriminant Δ and represents Δ.

THUS $\Phi: Cl^+(\Delta) \longrightarrow (\mathbb{Z}/\Delta\mathbb{Z})^\times / H$ IS NOT SURJECTIVE. THEN, THERE ARE AT MOST $2^{\mu-1}$ GENERA

$$\Phi': Cl^+(\Delta) \longrightarrow\!\!\!\!\rightarrow \ker\chi / H \text{ is surjective}$$

Theorem THE PRINCIPAL GENUS CONSISTS OF THE CLASSES IN $\underbrace{Cl^+(\Delta)^2}_{\text{subgroup of squares in } Cl^+(\Delta)}$ AND THE NUMBER OF GENERA IS $2^{\mu-1}$

Proof

- We note that $\ker\chi$ has index 2 in $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ (IT IS A KNOWN FACT THAT SQUARES ARE OF INDEX 2) $\Rightarrow \ker\chi/H$ has order $2^{\mu-1}$. Since Φ' is surjective $\Rightarrow Cl^+(\Delta)$ has at least $2^{\mu-1}$ genera $\Rightarrow$ exactly $2^{\mu-1}$ genera

- We have a homomorphism $\Phi': Cl^+(\Delta) \longrightarrow \ker\chi/H \longrightarrow \{\pm 1\}^{\mu-1}$
IT follows $(Cl^+(\Delta))^2 \subseteq \ker\Phi'$
$$\downarrow$$
$$\varphi: Cl^+(\Delta)/Cl^+(\Delta)^2 \longrightarrow \{\pm 1\}^{\mu-1}$$
squaring gives:
$$0 \longrightarrow \underbrace{Cl^+(\Delta)_0}_{\text{ELEMENTS OF ORDER} \le 2} \longrightarrow Cl^+(\Delta) \longrightarrow Cl^+(\Delta)^2 \longrightarrow 0$$
$\Rightarrow [C : C^2] = \#C_0 = 2^{\mu-1}$ (Prop 3.11)

Thus φ is an isomorphism (we know surjectivity and now $\#\frac{Cl^+(\Delta)}{Cl^+(\Delta)^2} = \#\{\pm 1\}^{\mu-1}$
Hence, $Cl^+(\Delta)^2 = \ker\Phi' =$ PRINCIPAL GENUS.

SOME EXAMPLES.

- WHEN IS $p = x^2 + 2y^2$? Quadratic form of discriminant -8. How many reduced quadratic forms of discriminant -8 are there?

REDUCED MEANS $|b| \le a \le c$ and $b \ge 0$ if $|b| = a$ OR $a = c$

$\Delta = -8 \le a^2 - 4a^2 = -3a^2$ $\quad 3a^2 \le 8 \Rightarrow a = 0 \Rightarrow b = 0$ ↯

$a = 1$

$a = 1$ implies $b = 0, 1$ if $b = 1 \Rightarrow -8 = 1 - 4c$ ↯ IN $\mathbb{Z} \Rightarrow b = 0$

$\Rightarrow -8 = -4c \Rightarrow c = 2 \Rightarrow$ THERE IS A UNIQUE REDUCED FORM.

$\#Cl^+(-8) = 1$ $\quad \langle 1, 0, 2 \rangle$. A prime is represented by a form of discriminant $-8 \iff$ it is represented by the principal form $\iff \left(\frac{-8}{p}\right) = 1$

$\left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = 1 \iff \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$

$\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p^2+4p-5}{8}} = 1 \iff \frac{p^2+4p-5}{8} = 2k$

$p^2 + 4p - 5 = 16k$ $\quad p^2 + 4p - 5 \equiv 0 \bmod 8 \Rightarrow p \equiv 1, 3 \bmod 8$

FINALLY $p = x^2 + 2y^2 \iff p \equiv 1, 3 \bmod 8$

- $p = x^2 + 3y^2$? QUADRATIC FORM of discriminant -12

$\#Cl(-12) = 1$: $\langle 1, 0, 3 \rangle$

$p = x^2 + 3y^2 \iff \left(\frac{-12}{p}\right) = 1$ $\qquad \left(\frac{-12}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$

$\left(\frac{-12}{p}\right) = 1 \iff \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1$

Observe that $\left(\frac{q}{p}\right) = 1 \iff p = \pm\beta^2 \bmod 4q$ some odd integer β

So $\left(\frac{3}{p}\right) = 1 \iff p$ is a square mod $12 \iff p \equiv \pm 1, \pm 9 \bmod 12$

$p \equiv$	1	5	7	11
$(-1/p)$	+	+	−	−
$(3/p)$	+	−	−	+

$p = x^2 + 3y^2 \iff p \equiv 1 \bmod 3$

$(\iff p \equiv 1, 7 \bmod 12)$

- WHEN IS $p = x^2 + 5y^2$? $\Delta = -20$ $\quad a = 0 \Rightarrow b = 0$ ↯; $a = 1 \Rightarrow b = 0$, ✗ $\rightsquigarrow \langle 1, 0, 5 \rangle$; $a = 2 \Rightarrow b = \cancel{0}, \cancel{\pm 1}, 2 \rightsquigarrow \langle 2, 2, 3 \rangle$

$Cl^+(-2) \simeq C_2 = \{\langle 1, 0, 5 \rangle, \langle 2, 2, 3 \rangle\}$

they live in different genera since $\mu = 2$

Now p is represented by a form of disc $-20 \iff \underline{p \equiv 1, 9 \ (\langle 1, 0, 5 \rangle) \text{ or } 3, 7 \ (\langle 2, 2, 3 \rangle)}$

Remark this procedure will give us a full solution to the question of when a prime is of the form $x^2 + ny^2 \iff$ the principal genus consists precisely of the principal class (WHEN $Cl(D)$ IS AN ELEMENTARY ABELIAN 2-GROUP)