Álgebra Moderna II : 30 de mayo

Clase pasada: Formas binarias y
la acción en ellas de $SL(2,\mathbb{Z})$.

Hoy: Formas binarias reducidas
y el número de clase h_D.

$$f(x,y) = ax^2 + bxy + cy^2 \qquad a,b,c \in \mathbb{Z}.$$

↳ primitiva si todos sus coeficientes
son primos relativos

si $m \in \mathbb{Z}$ & $m = f(x,y)$ para algunos

$x, y \in \mathbb{Z}$ entonces m es representado por

la forma f. (si $(x,y) = 1$, diremos

que la representación es

propia).

Dos formas $f(x,y)$ & $g(x,y)$ son equivalentes

si existen enteros r, s, u, v con $\begin{vmatrix} r & s \\ u & v \end{vmatrix} = \pm 1$

t.q. $f(x,y) = g(rx+uy, sx+vy)$. $(f \sim g)$

Nota: si f es una forma primitiva &

$f \sim g$, entonces g es primitiva

EJER

Def: Si $f = A \cdot g$ con $|A| = 1$ decimos que f y g son propiamente equiv.

Cuando $|A| = -1$ les llamamos impropiamente equivalentes.

Eg: $ax^2 + bxy + cy^2 \xrightarrow{T} ax^2 - bxy + cy^2$

$T(x,y) = (x,-y)$. Impropiamente equivalentes.

¿Son propiamente equivalentes?

↳ (Sí $2x^2 \pm 2xy + 3y^2$)

(no $3x^2 \pm 2xy + 5y^2$)

Proposición: $f(x,y)$ representa a $m \in \mathbb{Z}$ propiamente ssi f es propiamente equivalente a $g(x,y) = mx^2 + Bxy + Cy^2$ $B, C \in \mathbb{Z}$.

Demostración: $f(p,q)=m$ con $(p,q)=1$

encontramos $r,s\in\mathbb{Z}$ tal que $\begin{vmatrix} p & q \\ r & s \end{vmatrix}=1$.

Entonces
$$f(x,y)=ax^2+bxy+cy^2$$
$$=f(px+ry,\ qx+sy)$$
$$=f(p,q)x^2+(\quad)xy+f(r,s)y^2.$$

El recíproco es sencillo. $\boxtimes$

Recordar que si $f\sim g$ entonces ambas formas tienen el mismo discriminante.

<u>Proposición</u>: Sea $D\equiv 0,1 \pmod 4$ & $m\in\mathbb{Z}$ impar con $(D,m)=1$.

Entonces, m es representado propiamente por una forma binaria primitiva $\underline{\text{ssi}}$ de discriminante D

$\left(\frac{D}{m}\right)=1$; D es residuo cuadrático modulo m.

Demostración: si $m = f(x,y)$ propiamente

$\Rightarrow$ $f(x,y) \underset{\substack{\uparrow \\ \text{propia}}}{\sim} mx^2+Bxy+Cy^2$. $\Rightarrow$ $\underbrace{D=B^2-4mC}_{D\equiv B^2 \pmod m}$

Reciprocamente, $D\equiv B^2 \pmod m$. Como $m\in\mathbb{Z}$ es impar, podemos asumir D & B tienen la misma paridad. Entonces

EJERCICIO

$$D\equiv 0,1 \pmod 4 \Rightarrow$$

$$D\equiv B^2 \pmod{4m}$$

$\Rightarrow$ $D=B^2-4mC$ para algún $C\in\mathbb{Z}$, & $\underbrace{mx^2+Bxy+Cy^2}_{\text{Discri}=D}$. $\blacksquare$

COROLARIO: $n \in \mathbb{Z}$ y p entero primo $(\neq 2)$ con $(n,p)=1$.

Entonces, $\left(\frac{-n}{p}\right)=1$ <u>ssi</u> p es representable por una forma primitiva de discriminante de discriminante $-4n$.

Demostración: $$\left(\frac{-4n}{p}\right) \underset{\text{EJER}}{=} 1 \underset{\text{EJER}}{=} \left(\frac{-n}{p}\right).$$ ∎

Este corolario: $\left(\frac{-3}{13}\right)=1$ entonces 13

$$13 = 13x^2+12xy+3y^2 \quad , \quad D=-12.$$

Recordar: ¿Qué primos se pueden escribir como $p=x^2+y^2$? ó

¿$p=x^2+2y^2$? ó ¿$p=x^2+3y^2$?

Def (Lagrange) / Una forma primitiva y positiva definida* se llama <u>reducida</u> si $|b| \leq a \leq c$ y $b \geq 0$ si $\begin{cases} |b| = a \\ \text{ó} \\ a = c \end{cases}$.

Eg: x^2+y^2 ; x^2+2y^2 ; x^2+3y^2 ; x^2+my^2 $m>0$

$2x^2+2xy+3y^2$, $3x^2 \pm 2xy+5y^2$, ...

<u>Teorema:</u> Toda forma primitiva y definida positiva es propiamente equivalente a una única forma reducida.

Demostración: 1) Probemos que una forma dada es equivalente (propiamente) a una que satisface $|b| \leq a \leq c$.

*) escojamos la forma $\overset{f}{\vee}$ con $|b|$ tan pequeño como sea posible.

(si $a < |b|$, entonces $f(x+my, y) = ax^2 + (2am+b)xy + c'y^2$.
y podemos escojer $m \in \mathbb{Z}$
tal que $|2am+b| < |b|$ que contradice la elección de f). Entonces $|b| < a$ & $|b| < c$.

**) si $a > c$, aplicamos $T(x,y) = (-y, x)$

Al final tenemos $|b| < a < c$.

2) Demostremos que dicha forma es equiv. (prop) a una reducida.

*) si $b < 0$ & $a = -b$ ó $a = c$

entonces $ax^2 - bxy + cy^2$ es reducida.

Por lo tanto, tenemos que probar que

las formas $ax^2+bxy+cy^2$ y

$ax^2-bxy+cy^2$

son propiamente equivalentes:

$a=-b$; $(x,y)\mapsto(x+y,y)$

$ax^2+(-a)xy+cy^2 \mapsto ax^2+ayx+cy^2$

$a=c$; $(x,y)\mapsto(-y,x)$

$(a,b,a)\longmapsto(a,-b,a)$

3) UNICIDAD: VER DAVID COX,
primes of the form x^2+ny^2
pág: 26.

Eg: $3x^2 \pm 2xy + 5y^2$ son equivalentes pero ambas son <u>reducidas</u>; por lo tanto NO pueden ser propiamente equivalentes.

Eg: $2x^2 \pm 2xy + 3y^2$ sólo $2x^2 + 2xy + 3y^2$ es reducida $(a = |b|)$ & $2x^2 - 2xy + 3y^2$ es propiamente equivalente a $(2,2,3)$.

<u>OBSERVACIÓN</u>: si (a,b,c) es reducida de disc $D<0$, entonces $b^2 \leq a^2$ & $a \leq c$ $\Rightarrow$

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$$

$\Rightarrow$

$$a \leq \sqrt{-D/3}$$

$\Rightarrow$ con D fijo sólo hay una cantidad finita de valores (a,b,c) con $|b| \leq a$ & $a \leq \sqrt{-D/3}$ $\Rightarrow$ ¡c está acotado!

<u>Teorema:</u> Con $D<0$ fijo. El número $h(D)$ de clases primitivas definidas positivas de discriminante D, es finito. Más aún,

$$h(D) = \#\{\text{formas reducidas de discriminante } D\}$$

D	$h(D)$	formas reducidas
-4	1	x^2+y^2
-8	1	x^2+2y^2
-12	1	x^2+3y^2
-20	2	x^2+5y^2 ; $2x^2+2xy+3y^2$
-28	1	x^2+7y^2