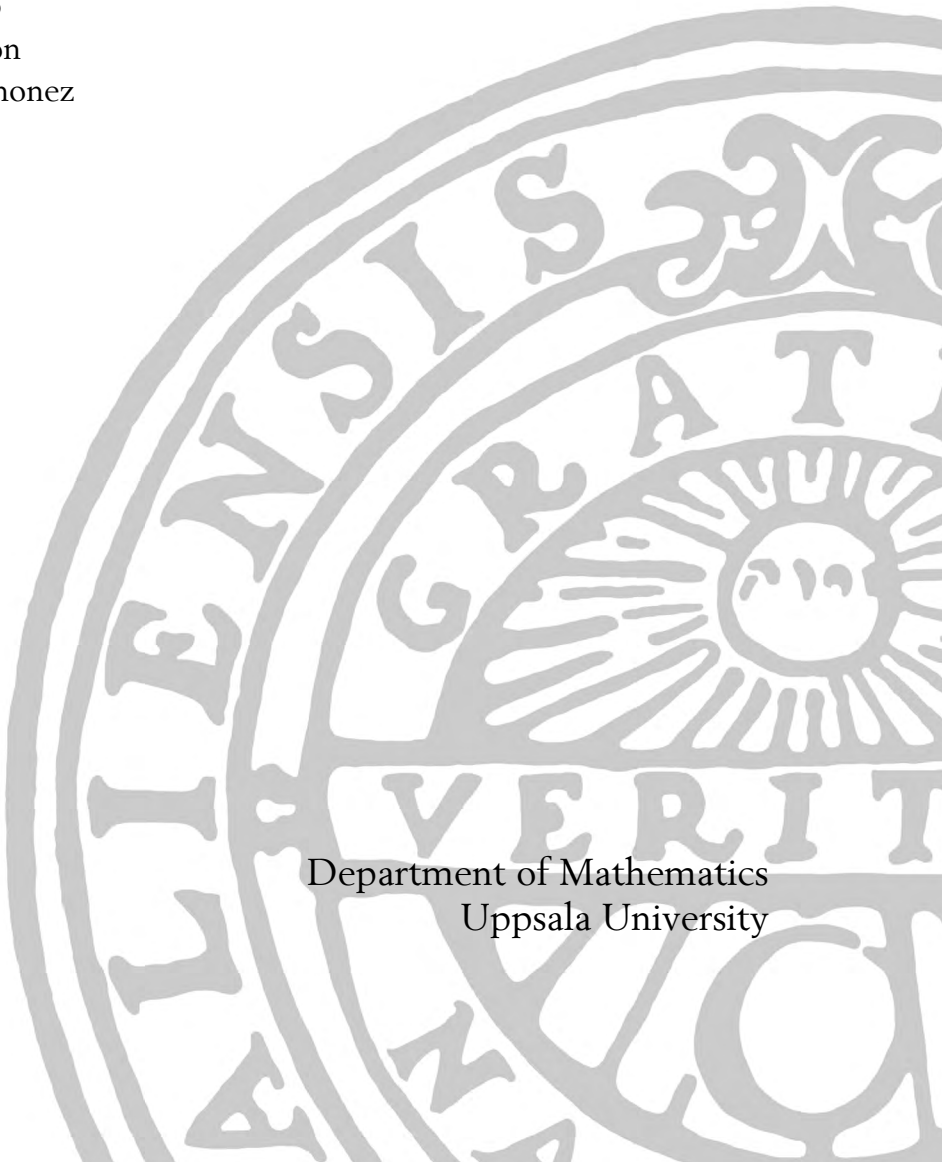
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2016:14

# Binära kvadratiska former

Vasam Mazraeh

Examensarbete i matematik, 15 hp
Handledare: Andreas Strömbergsson
Examinator: Veronica Crispin Quinonez
Juni 2016



Department of Mathematics
Uppsala University

# *Innehållsförteckning*

## *Inledning*

Under många år försökte Euler hitta bevis för Fermats satser om binära kvadratiska former. Liksom Euler har flera andra gjort samma försök bland annat Gauss, Legendre och Lagrange. Som följd av deras arbete och fördjupningar skapades teorin om binära kvadratiska former men äran gick till en av dem nämligen Lagrange; han anses vara den som skapade ämnet binära kvadratiska former.

Teorin om summan av kvadrater startade en ny värld inom talteori. För att förstå hur ämnet *binära kvadratiska former* skapades måste vi titta på Fermats och Lagranges verk.

Fermats satser om summan av två kvadrater handlar om vilka primtal som kan skrivas på formen $p = x^2 + y^2$. Svaret är att detta går för $p = 2$ och för alla primtal $p \equiv 1\ (mod\ 4)$, men inte för några andra primtal. Till en början var $x^2 + y^2$en av få former som Fermat arbetade med. Under tidens gång lyckades Fermat bevisa liknande resultat även för några andra former såsom $p = x^2 + 2y^2$ (svaret är att detta går om och endast om $p = 2$ eller $p \equiv 1\ eller\ 3\ (mod\ 8)$), och $p = x^2 + 3y^2$ (svaret är att detta går om och endast om $p = 3$ eller $p \equiv 1\ (mod\ 3)$). Fermat fortsatte imponera med liknande upptäckter tills han stötte på ett stort problem; han misslyckades nämligen med att karaktärisera de primtal som kan skrivas på formen $p = x^2 + 5y^2$. Orsaken till misslyckandet var okänd och förblev så under hela tvåhundra år tills Lagrange gjorde en fascinerande upptäckt år 1773.

Lagrange var en mycket framgångsrik matematiker. Efter många års arbete inom talteorin lyckades Lagrange utveckla en generell teori för *binära kvadratiska former med heltalskoefficienter*, dvs. funktioner av typen $f(x, y) = ax^2 + bxy + cy^2$, där $a, b, c \in \mathbb{Z}\ h\ x, y$ är två variabler med egenskapen $x, y \in \mathbb{Z}$.

Fermats satser om summan av kvadrater och primtalen kunde så småningom utvidgas till generella fall, dvs. man kunde beskriva vilka primtal som kan framställas med en given kvadratisk form. Efter ett långt och avancerat arbete med en mängd av beräkningar av olika binära kvadratiska former konstaterade Lagrange att många av formerna var ekvivalenta. Dvs. de har ett samband med varandra via variabelbyten.

Exempelvis, betrakta den kvadratiska formen $x^2 + y^2$. Låt oss här substituera $x = u + v$ och $y = v$; vi får då den kvadratiska formen $(u + v)^2 + v^2 = u^2 + 2uv + 2v^2$. En central observation är nu att de två formerna $x^2 + y^2$och $u^2 + 2uv + 2v^2$ kan representera precis samma heltal. Varför? Det är uppenbart ur vår konstruktion att varje heltal som kan uttryckas som $u^2 + 2uv + 2v^2$ även kan skrivas som $x^2 + y^2$, nämligen genom att sätta $x = u + v$ och $y = v$. Men vi har också omvänt att för givna heltal $x, y$, om vi sätter $u = x - y$ och $v = y$ så blir $x = u + v$ och $y = v$, och därmed $(u + v)^2 + v^2 = u^2 + 2uv + 2v^2$, dvs. varje tal som kan uttryckas som $x^2 + y^2$ kan även skrivas som $u^2 + 2uv + 2v^2$, och vårt påstående är bevisat.

Alla former som kan överföras i varandra via sådana variabelbyten kallas ekvivalenta, därför att sådana former kan representera precis samma uppsättning av heltal. Lagrange visste att de transformationerna

$$x = au + bv$$
$$y = cu + dv$$

som leder till ekvivalenta former är precis de som uppfyller $ad - bc = \pm 1, a, b, c, d\ \in \mathbb{Z}$. Sådana transformationer kallas *unimodulära*. Lagrange använde sig av dessa transformationer

för att hitta den enklaste formen i en samling av ekvivalenta former. Med sina arbeten och upptäckter lyckades Lagrange utveckla mycket effektivare bevis för Fermats satser än Fermats egna bevis.

Detta arbete kommer att handla om teorin för binära kvadratiska former. Vi kommer att studera olika begrepp inom ämnet, såsom *ekvivalens och reduktion av binära kvadratiska former*, *summan av två kvadrater* och *positivt definita binära kvadratiska former* mm.

# *1 Binära kvadratiska former*

En binär kvadratisk form är ett homogent polynom av grad två i två variabler. I detta arbete kommer vi bara att vara intresserade av former med *heltalskoefficienter*. Vi gör alltså följande definition.

**Definition 1**
En *binär kvadratisk form* är en funktion i två variabler av typen

$$f(x,y) = ax^2 + bxy + cy^2, \quad \text{där } a,b,c \text{ är } heltal.$$

**Exempel 1:**

1) $f(x,y) = x^2 + 2xy + y^2$
2) $f(x,y) = 16x^2 + 48xy + 36y^2$

## 1.1 Diskriminant

Ett tal är en *perfekt kvadrat* (eller kvadrat) om det kan skrivas på formen $n^2$, där $n$ är ett heltal.

**Exempel 2:**
$1, 4, 9, 16 \; och \; 121$ är kvadrater.
$2, 3, 5, 120,$ är ej kvadrater.

**Definition 2**
*Diskriminanten* till den kvadratiska formen $f(x,y) = ax^2 + bxy + cy^2$ definieras som $d = b^2 - 4ac$.

**Exempel 3:**
Bestäm diskriminanten till $f(x,y) = 14x^2 + 15xy + 7y^2$.

**Lösning:**
$a = 14, b = 15 \; och \; c = 7 \; ger$:
$d = b^2 - 4ac = 15^2 - 4 \cdot 14 \cdot 7 = 225 - 392 = -167.$

**Sats 1**
En binär kvadratisk form $f$ kan skrivas som en produkt av två linjära former med heltalskoefficienter om och endast om $d$ är en *perfekt kvadrat*.

**Bevis:**
Vi ska visa att om $d$ är en perfekt kvadrat (eventuellt noll) så finns det $u_1, u_2, v_1, v_2 \in \mathbb{Z}$ så att $f(x,y) = (u_1x + v_1y)(u_2x + v_2y)$.
Anta att $a = 0$. Då är $f(x,y) = ax^2 + bxy + cy^2 = bxy + cy^2 = y(bx + cy)$ en faktorisering i två linjära former med heltalskoefficienter, där $u_1 = 0, u_2 = b, v_1 = 1, v_2 = c$.

Låt nu $a \neq 0$ och låt $h(t) = t^2 + \frac{b}{a}t + \frac{c}{a} \in \mathbb{Q}[t]$. Enligt antagandet är diskriminanten en perfekt kvadrat dvs. $d = b^2 - 4ac = n^2$ för något heltal $n$. Vi kan nu enligt konjugatregeln skriva ekvationen som två linjära faktorer i $\mathbb{Q}[t]$ som $h(t) = (t - \frac{-b+n}{2a})(t - \frac{-b-n}{2a})$.
Nu har vi att:

$$f(x,y) = ay^2 h\left(\frac{x}{y}\right) = \frac{(ax - \frac{-b+n}{2}y)(ax - \frac{-b-n}{2}y)}{a}.$$

Eftersom $b + n = b - n + 2n$. Så gäller att $b - n \equiv 0\ (mod\ 2)$ om och endast om $b + n \equiv 0\ (mod\ 2)$. Enligt kongruenslagarna ska produkten av dem också vara kongruent med 2. D.v.s. $(b+n)(b-n) = b^2 - n^2 = 4ac \equiv 0\ (mod\ 2)$ vilket medför att båda faktorerna är delbara med 2.
Låt nu $w = \frac{-b-n}{2}$. Vi har att:

$$f(x,y) = \frac{(ax - wy)(ax - (w+n)y)}{a}.$$

Från $f(0,1) = c$ ser vi att $w(w+n) = ac$. Låt nu $s = (a,w)$ och $a = sz$. På samma sätt som $a|w(w+n)$, delar $z$ också $w(w+n)$. Vidare är $(z,w) = 1$ vilket medför att $z|(w+n)$. Vi har sett att $a$ kan skrivas som $a = sz$ så att $sr = w$ och $zl = w + n$ där $l, r, s, z \in \mathbb{Z}$. Så

$$f(x,y) = \left(zx - \frac{w}{s}y\right)\left(sx - \frac{w+n}{z}\right).$$

Vi utelämnar beviset för omvändningen.■

**Exempel 4:**

1) $f(x,y) = 4y^2 = (0 + 2y)(0 + 2y)$
   $a = b = 0, \quad c = 4$
   $d = b^2 - 4ac = 0^2 - 4 \cdot 0 \cdot 4 = 0$, som är en perfekt kvadrat.

2) $f(x,y) = 6x^2 - 32xy + 42y^2 = (3x - 7y)(2x - 6y)$
   $a = 6, \quad b = -32, \quad c = 42$
   $d = b^2 - 4ac = (-32)^2 - 4 \cdot 6 \cdot 42 = 16$, som är en perfekt kvadrat.

**Sats 2**
Låt $f(x,y) = ax^2 + bxy + cy^2$ vara en binär kvadratisk form med $a, b, c \in \mathbb{Z}$ och diskriminant $d$. Då har $f(x,y) = 0$ endast en heltalslösning, $x = y = 0\ om\ d$ inte är en perfekt kvadrat. När detta gäller är även $a \neq 0\ och\ c \neq 0$.

**Bevis:**
Anta att $a \neq 0$ och $c \neq 0$, ty om $a = 0$ eller $c = 0$ då får vi att $ac = 0$, vidare blir diskriminanten $d = b^2 - 4ac = b^2 - 4 \cdot 0 \cdot 0 = b^2$ som är en perfekt kvadrat.
Anta att $x_0$ och $y_0$ är två heltal så att $f(x_0, y_0) = 0$. Om $y_0 = 0$ så $ax_0 = 0$ men $a \neq 0$ så $x_0 = 0$, på samma sätt får vi att $x_0 = 0$ medför att $y_0 = 0$. Om $x_0 \neq 0$ och $y_0 \neq 0$ kvadratkompletterar vi $4af(x,y) = (2ax + by)^2 - dy^2$ och får att $(2ax_0 + by_0)^2 = d{y_0}^2$ eftersom $f(x_0, y_0) = 0$. Men $d{y_0}^2 \neq 0$ och enligt den unika faktoriseringen är $d$ en perfekt kvadrat. ■

**Exempel 5:**
Betrakta $f(x,y) = 3x^2 + 2xy + y^2$. Vi beräknar diskriminanten och får:

$d = b^2 - 4ac = 2^2 - 4 \cdot 3 \cdot 1 = 4 - 12 = -8$, som ej är en perfekt kvadrat.

Enligt **sats 2** är $(x,y) = (0,0)$ den enda heltalslösningen till $f(x,y) = 0$.

## 1.2 Indefinita och definita kvadratiska former

Vi ska nu studera vissa egenskaper hos binära kvadratiska former nämligen indefinit, positivt semidefinit och negativt semidefinit.

**Definition 3: Indefinit**
En binär kvadratisk form $f(x,y)$ kallas indefinit om det finns $x, y$ så att $f(x,y) > 0 \; och$ om det $finns \; x, y \; så \; att \; f(x,y) < 0$, d.v.s. om den antar både positiva och negativa värden. Den kallas positivt semidefinit om $f(x,y) \geq 0$ för alla $x, y$ och negativt semidefinit om $f(x,y) \leq 0$ för alla $x, y$. En semidefinit form kallas definit om $f(x,y) = 0$ endast för $x = 0 \; och \; y = 0$.

**Exempel 6:** Indefinit
$f(x,y) = \; x^2 - 18y^2$
$f(5,1) = \; 5^2 - 18 \cdot 1^2 = \; 7$
$f(1,5) = \; 1^2 - 5 \cdot 5^2 = -124$

**Exempel 7:** Positivt semidefinit men inte definit
$f(x,y) = 25x^2 - 50xy + 25y^2$
Den är inte definit ty,
$f(2,2) = \; 25 \cdot 2^2 - 50 \cdot 2 \cdot 2 + 25 \cdot 2^2 \; = \; 100 - 200 + 100 \; = \; 0.$
Den är positivt semidefinit ty,
$f(x,y) = 25(x-y)^2 \geq 0$ för alla $x, y$.

Vi kan med hjälp av diskriminanten avgöra om en binär kvadratisk form är definit eller indefinit.

**Sats 3**
Låt $f(x,y) = ax^2 + bxy + cy^2$ vara en binär kvadratisk form med heltalskoefficienter och diskriminant $d$. Då gäller att:
$f(x,y)$ är indefinit om $d > 0$.
$f(x,y)$ är semidefinit men inte definit om $d = 0$.
$f(x,y)$ är positivt definit om $a > 0$ och $d < 0$.
$f(x,y)$ är negativt definit om $a < 0$ och $d < 0$.
Om $f(x,y)$ är positivt definit så är $-f(x,y)$ negativt definit.
Om $f(x,y)$ är definit så har $a$ och $c$ har samma tecken.

**Bevis:**
Anta att $d > 0$. Då är $f(1,0) = a$ och $f(b,-2a) = -ad$. På samma sätt är $f(0,1) = c$ och $f(-2c,b) = -cd$.

För $a = c = 0$ gäller att om $d = b^2 > 0$ så är $b \neq 0$ som medför att $f(1,1) = b$ och $f(1,-1) = -b$, dvs. $f$ tar både positivt och negativt tecken.
Anta nu att $d = 0$ och $a \neq 0$. Pga. $4af(x,y) = (2ax + by)^2 - dy^2$ gäller då att alla nollskilda värden för $f(x,y)$ har samma tecken som $a$. D.v.s. $f(x,y)$ är semidefinit.
Vidare $f(b,-2a) = -ad = 0$ men eftersom $a \neq 0$ så är $f$ inte definit.
Om $a = 0$ så $d = b^2$ som medför att $b = 0$ eftersom $d = 0$. Om $f(x,y) = cy^2$ så har alla nollskilda värden samma tecken som $c$ men $f$ är inte definit eftersom $f(1,0) = 0$.
Slutligen om $d < 0$ så medför **sats 2** tillsammans med $4af(x,y) = (2ax + by)^2 - dy^2$ att $4af(x,y) > 0$ för alla heltal $x \neq 0$ och $y \neq 0$. Därmed är$f$ definit eftersom $f(1,0) = a$ och $f(0,1) = c$. Nu kan vi dra slutsatsen att $a$ och $c$ har samma tecken, positivt för positivt definit och negativt för negativt definit. ■

Ett givet heltal $d$ är diskriminant till en binär kvadratisk form om det uppfyller kraven i **sats 4** nedan.

**Sats 4**
Låt $d$ vara ett givet heltal. Då finns det minst en binär kvadratisk form med heltalskoefficienter och diskriminant $d$ om och endast om $d \equiv 0$ eller 1 (mod 4).

**Bevis:**
Vi vet att $d = b^2 - 4ac$, vilket medför $d \equiv b^2 (mod\ 4)$. Eftersom för varje heltal $b$ gäller att $b^2 \equiv\ 0\ eller\ 1\ (mod\ 4)$, så medför det att diskriminanten
$d = b^2 - 4ac\ \equiv\ 0\ eller\ 1\ (mod\ 4)$.
Omvänt, anta att $d \equiv 0\ (mod\ 4)$. Det kan vi skriva som $d = 4ac$, vi löser ut $c$ och får att $c = \frac{d}{4a}$. Då har formen $f(x,y) = x^2 - \left(\frac{d}{4}\right)y^2$ med $a = 1, b = 0\ och\ c = \frac{d}{4}$ insatta, diskriminanten $d$. På samma sätt om $d \equiv 1$ (mod 4) så har formen
$f(x,y) = x^2 + xy - (\frac{d-1}{4})y^2$ med $a = 1, b = 1\ och\ c = \frac{d-1}{4}$ insatta, diskriminant $d$.

## 1.3 Representationer av heltal

Vi säger att en kvadratisk form $f(x,y)$ *representerar* ett heltal $n$ om det finns två heltal $x_0$ och $y_0$ så att $f(x_0,y_0) = n$. En sådan representation kallas *proper* om $sgd(x_0,y_0) = 1$; annars improper. Om $f(x_0,y_0) = n$ och $sgd(x_0,y_0) = g$ så gäller att $g^2|n$, $sgd(\frac{x_0}{g},\frac{y_0}{g}) = 1$ och $f\left(\frac{x_0}{g},\frac{y_0}{g}\right) = \frac{n}{g^2}$.

Vi ska nu studera alla heltal $n$ som *representeras* respektive *propert representeras* av en given kvadratisk form. Vi ska också studera om $n$ kan representeras av en kvadratisk form med en given diskriminant. Det gör vi i **sats 5** nedan.

**Sats 5**
Låt $n$ och $d$ vara givna heltal med $n \neq 0$. Då finns det en binär kvadratisk form med diskriminant $d$ som representerar $n$ propert om och endast om kongruensekvationen $x^2 \equiv d\ (mod\ 4|n|)$ har en lösning $x$.

**Bevis:**
Låt $b$ vara en lösning till $x^2 = d\ (mod\ 4|n|)$ så att $b^2 - d = 4nc$. Då har

$f(x,y) = nx^2 + bxy + cy^2$ heltalskoefficienter och diskriminant $d$. Vidare är $f(1,0) = n$ en proper representation av $n$, för $x = 1\ och\ y = 0$.
Omvänt, låt $f(x_0, y_0)$ vara en proper representation av $n$ med formen $f(x,y) = ax^2 + bxy + cy^2$, med diskriminant $d = b^2 - 4ac$. Vi har att $sgd(x_0, y_0) = 1$, välj heltal $m_1\ och\ m_2$ så att $m_1 \cdot m_2 = 4|n|$, $sgd(m_1, y_0) = 1$ och $sgd(m_2, x_0) = 1$. Låt exempelvis $m_1$ vara produkten av alla primtalspotenserna $p^\alpha$ i $4n$ så att $p|x_0$ och $m_2 = \frac{4|n|}{m_1}$. Då ger $4af(x,y) = (2ax + by)^2 - dy^2$ att $4an = (2ax_0 + by_0)^2 - d{y_0}^2$ som medför att $(2ax_0 + by_0)^2 \equiv d{y_0}^2\ (mod\ m_1)$.
Pga. $sgd(y_0, m_1) = 1$ finns det ett heltal $\bar{y}_0$ med egenskapen $y_0\bar{y}_0 \equiv 1(mod\ m_1)$. Det följer att kongruensekvationen $u^2 \equiv d\ (mod\ m_1)$ har en lösning $u = u_1 = (2ax_0 + by_0)\bar{y}_0$. På samma sätt om vi byter plats på $a$, $c$ och $x, y$, finner vi att kongruensekvationen $u^2 \equiv d(mod\ m_2)$ har en lösning $u = u_2$. Slutligen ger kinesiska restsaten ett heltal $w$ med egenskapen $w \equiv u_1(mod\ m_1)\ och\ w \equiv u_2(mod\ m_2)$, därför $w^2 = {u_1}^2 \equiv d\ (mod\ m_1)$. På samma sätt $w^2 = {u_2}^2 \equiv d(mod\ m_2)$ som tillsammans ger $w^2 \equiv d(mod\ m_1 m_2)$ där $m_1 m_2 = 4n$. ■

**Obs:**
$a$ är en *kvadratisk rest* $(mod\ p)$ betyder att om det finns $x \in \mathbb{Z}$ så att $x^2 \equiv a\ (mod\ p)$.

**Sats 6: Eulers Kriterium**
Låt $p$ vara ett udda primtal och låt $a$ vara ett heltal sådant att $p \nmid a$. Då är $a$ en *kvadratisk rest* till $p$ om $a^{(p-1)/2} \equiv 1\ (mod\ p)$ och en *icke-kvadratisk rest* om $a^{(p-1)/2} \equiv -1\ (mod\ p)$.

**Bevis:**
Låt m vara en primitiv rot (mod p).
Om $a$ är en kvadratisk rest $(mod\ p)$ så är $a = m^{2k}$, som medför att $a^{(p-1)/2} = m^{k(p-1)} = (m^{p-1})^k = 1$.
Om $a$ är en icke-kvadratisk rest $(mod\ p)$ så är $a = m^{2k+1}$, som medför att $a^{(p-1)/2} = m^{k(p-1)} \cdot m^{(p-1)/2} = m^{(p-1)/2}$.
Nu har vi **enligt Fermats lilla sats** att $m^{(p-1)/2} = \pm 1$, men $m^{(p-1)/2} = 1$ är omöjligt eftersom $m$ är en primitiv rot. Därför är $a^{(p-1)/2} = -1$ om $a$ är en icke-kvadratisk rest. ■

**Exempel:**
Avgör om kongruensekvationen $x^2 \equiv 5\ (mod\ 37)$ har lösningar eller inte.

**Lösning:**
Vi ser att 37 är ett udda primtal som inte delar 5. Nästa steg är att avgöra om $5^{18}$ är kongruent med 1 eller $-1\ (mod\ 37)$.

$$\begin{aligned} 5 &\equiv 5\ (mod\ 37) \\ 5^2 &\equiv 25\ (mod\ 37) \\ 5^4 = (25)^2 = 625 &\equiv 33\ (mod\ 37) \\ 5^8 = (33)^2 = 1089 &\equiv 16\ (mod\ 37) \\ 5^{16} = (16)^2 = 256 &\equiv 34\ (mod\ 37) \\ 5^{18} = 5^{16} \cdot 5^2 \equiv (34) \cdot (25) = 36 &\equiv -1\ (mod\ 37) \end{aligned}$$

Eftersom $5^{18} \equiv -1\ (mod\ 37)$, så medför **Eulers Kriterium** att $x^2 \equiv 5\ (mod\ 37)$ saknar lösningar.

**Definition 4: Legendresymbolen**
Låt $p$ vara ett udda primtal och låt $a$ vara ett godtyckligt heltal. Då definieras Legendresymbolen $\left(\frac{a}{p}\right)$ så här:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & om\ a\ \text{är}\ en\ kvadratisk\ rest\ (mod\ p) \\ -1 & om\ a\ \text{är}\ en\ ickekvadratisk\ rest\ (mod\ p) \\ 0 & om\ p|a \end{cases}$$

## 1.4 Kvadratisk reciprocitet

**Sats 7**
Låt $p$ och $q$ vara udda primtal och låt $a, b$ vara två godtyckliga heltal. Då gäller:

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}\ (mod\ p)$

(ii) $a \equiv b\ (mod\ p) \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

(iv) Om $sgd(a,p) = 1$, så är $\left(\frac{a^2}{p}\right) = 1$ och $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

(v) $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ om $p \equiv q \equiv 3\ (mod\ 4)$, annars $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

(vi) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1\ om\ p\ \equiv\ 1\ eller\ 7\ (mod\ 8) \\ -1\ om\ p\ \equiv\ 3\ eller\ 5\ (mod\ 8) \end{cases}$

(vii) $\left(\frac{1}{p}\right) = 1$ och $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1\ om\ p\ \equiv\ 1\ (mod\ 4) \\ -1\ om\ p\ \equiv\ 3\ (mod\ 4) \end{cases}$

**Bevis:**
**(i)** följer direkt av Eulers Kriterium.
**(ii)** Betrakta kongruensekvationen $x^2 \equiv a\ (mod\ p)$. Om ekvationen har/saknar lösningar så gäller det samma för $x^2 \equiv b\ (mod\ p)$ när $a \equiv b\ (mod\ p)$. (Exempel: Anta att kongruensekvationen $x^2 \equiv 5\ (mod\ 29)$ har lösningar. Det är samma ekvation som $x^2 \equiv 34\ (mod\ 29)$. Vidare måste Legendresymbolen $\left(\frac{5}{29}\right)$ vara lika med Legendresymbolen $\left(\frac{34}{29}\right)$.)

För **(iv)** betrakta kongruensekvationen $x^2 \equiv a^2\ (mod\ p)$. Det är uppenbart att ekvationen har lösning, nämligen $x = a$.
**(vii) Enligt Eulers Kriterium** $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2}\ (mod\ p)$. Låt $p \equiv 1\ (mod\ 4)$, där $p = 3{,}7{,}11$ ..., och låt $p$ vara ett tal bland dem. Då gäller att $(p-1)/2$ är ett jämnt tal, därför $\left(\frac{-1}{p}\right) \equiv 1\ (mod\ 4)$. Låt $p \equiv 3\ (mod\ 4)$, där $p = 5{,}13{,}19$ ... .,. Då gäller att $(p-1)/2$ är ett udda tal, vilket medför att $\left(\frac{-1}{p}\right) \equiv -1\ (mod\ 4)$.
Vi utelämnar bevisen för (**iii)** och för **(vi)**.■

**Exempel 9:**
Beräkna Legendresymbolen om $a = 1000$ och $p = 11$.

**Lösning:**
11 är ett udda primtal och dessutom är $11 \nmid 1000$; ok!
Nu primtalfaktoriserar vi 1000 och får:
$1000 = 2^3 \cdot 5^3$
**Enligt (iii):**

$$\left(\frac{1000}{11}\right) = \left(\frac{2^3}{11}\right) \cdot \left(\frac{5^3}{p}\right) = \left(\frac{2^2}{11}\right) \cdot \left(\frac{2}{11}\right) \cdot \left(\frac{5^2}{11}\right) \cdot \left(\frac{5}{11}\right)$$

**Enligt (iv):**

$$\left(\frac{2^2}{11}\right) = 1 \; och \left(\frac{5^2}{11}\right) = 1$$

Därför:

$$\left(\frac{1000}{11}\right) = \left(\frac{2}{11}\right) \cdot \left(\frac{5}{11}\right)$$

**Enligt (vi):**

$$\left(\frac{2}{11}\right) = -1, ty \; 11 \equiv 3 \; (mod \; 8)$$

Vi ser att $5 \equiv 1(mod 4) \; och \; 11 \equiv 3(mod 4)$.

**enligt (v):**

$$\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right)$$

Därför:

$$\left(\frac{1000}{11}\right) = (-1) \cdot \left(\frac{11}{5}\right)$$

**Enligt (ii),** $11 \equiv 1 \; (mod \; 5)$, därför:

$$\left(\frac{1000}{11}\right) = (-1) \cdot \left(\frac{1}{5}\right)$$

**Enligt (vii):**

$$\left(\frac{1}{5}\right) = 1$$

Därför:

$$\left(\frac{1000}{11}\right) = (-1) \cdot (1) = -1.$$

Legendresymbolen $\left(\frac{1000}{11}\right) = -1$. Alltså; kongruensekvationen $x^2 \equiv 1000 \; (mod \; 11)$ saknar lösningar eftersom $n = 1000$ är en icke-kvadratisk rest $(mod \; 11)$.

**Korollarium 1**
Anta att $d \equiv 0\ eller\ 1\ (mod\ 4)$ och låt $p$ vara ett udda primtal. Då finns det en binär kvadratisk form med diskriminant $d$ som representerar $p$, om och endast om $\left(\frac{d}{p}\right) = 1$.

**Bevis:**
Samtliga representationer av $p$ måste vara propra, därför om $p$ är representerat så är det propert representerat. **Sats 5** medför att $d$ är en kvadrat $(mod\ 4p)$, dvs. $\left(\frac{d}{p}\right) = 1$.

Omvänt, om $\left(\frac{d}{p}\right) = 1$ så är $d$ en kvadrat $(mod\ p)$. Enligt antagandet $d$ är en kvadrat $(mod\ 4)$ och $p$ är udda. Enligt kinesiska restsatsen är $d$ en kvadrat $(mod\ 4p)$, alltså följer det av **sats 5** att $p$ är propert representerat med någon form av diskriminant $d$.■

# *2 Ekvivalens och reduktion av binära kvadratiska former*

Låt $f(x,y) = x^2 + y^2$ och $g(x,y) = x^2 + 2xy + 2y^2$ vara två givna former. Observera att $f(x,y) = g(x-y,y)$ eller ekvivalent $g(x,y) = f(x+y,y)$.

Utifrån beräkningarna i (1) och (2) nedan, ser vi att alla tal som är representerade av $g$ representeras också av $f$, och omvänt. Vidare gäller att koordinaterna för punkten $(x,y)$ är heltal om och endast om koordinaterna för punkten $(x+y,y)$ är heltal, och omvänt. En punkt med heltalskoordinater kallas för *gitterpunkt*.

**Exempel:**

$g(3,4) = 9 + 24 + 32 = 65$
$g(3,4) = f(3+4,4) = f(7,4) = \ 49 + 16 = 65.$ (1)

Omvänt:

$f(7,4) = 49 + 16 = 65$
$f(7,4) = g(x-y,y) = g(7-4,4) = g(3,4) = \ 9 + 24 + 32 = 65.$ (2)

## 2.1 Matriser och avbildningar

**Sats 8**
Låt $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ vara en $2x2$ matris med reella värden och låt $\begin{pmatrix} u \\ v \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}$ $(*)$.
Från linjär algebra vet vi att $(*)$ betyder att:

$$\begin{cases} u = \ m_{11}x + m_{12}y \\ v = m_{21}x + m_{22}y \end{cases}$$

Då är påståendena nedan ekvivalenta:

1) Den linjära avbildningen $(*)$ definierar en permutation av gitterpunkterna.
2) Matrisen $M$ har heltalskoefficienter och determinant $det(M) = \pm 1$, där $det(M) = m_{11}m_{22} - m_{12}m_{21}$.

Sedan tidigare vet vi från linjär algebra att $(*)$ definierar en permutation i $\mathbb{R}^2$om och endast om $det(M) \neq 0$.

**Bevis:**
Först visar vi att (2) medför (1). Om $M$ har heltalskoefficienter så är $(u, v)$ en gitterpunkt när $(x, y)$ är en gitterpunkt.
Om $det(M) \neq 0$ så har $M$ en invers:

$$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix}$$

Om (2) är uppfylld så har inversen heltalskoefficienter. Då ges den inverterade avbildningen $(u, v) \rightarrow (x, y)$ av matrismultiplikationen:

$$\begin{pmatrix} x \\ y \end{pmatrix} = M^{-1} \begin{pmatrix} u \\ v \end{pmatrix}$$

Vi visar nu omvänt att (1) medför (2). Vi väljer en gitterpunkt, säg $(x, y) = (1,0)$, vidare ger (*) att $(u, v) = (m_{11}, m_{21})$. För att punkten ska vara en gitterpunkt så måste $m_{11}$ och $m_{21}$vara heltal. På samma sätt för $(x, y) = (0,1)$ får vi att $m_{12}$ och $m_{22}$ måste vara heltal.
Slutligen vi ska visa att $det(M) \neq 0$.
Låt $(u, v) = (1,0)$ vara en gitterpunkt. Då ger (1) att (*) är en surjektiv avbildning, då finns det en gitterpunkt $(x_1, y_1)$ så att $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = M \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$. På samma sätt finns det en $(x_2, y_2)$ så att $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = M \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$. Punkterna kan skrivas som en enda matris $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = M \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$ $(**)$.

Från linjär algebra vet vi att om $M$ och $N$ är två $nxn$ matriser så gäller det att $det(MN) = det(M) \cdot det(N)(***)$.
Eftersom vi fokuserar endast på $n = 2$, vi får att:

$det(MN) = det(M) \cdot det(N) =$
$(m_{11}n_{11} + m_{12}n_{21})(m_{21}n_{12} + m_{22}n_{22}) - (m_{21}n_{11} + m_{22}n_{21})(m_{11}n_{12} + m_{12}n_{22}) =$
$(m_{11}m_{22} - m_{21}m_{12})(n_{11}n_{22} - n_{21}n_{12})$.

Vi tillämpar det på $(**)$ och får:
$det(M)(x_1y_2 - x_2y_1) = 1$, med heltalsfaktorer eftersom HL i $(**)$ har heltalskoefficienter.
Alltså; $det(M)|1$. Därför är $\det(M) = \pm 1$.■

Vi har nu studerat matriser med $det(M) = \pm 1$, men från och med nu fokuserar vi endast på matriser med $det(M) = 1$.

## 2.2 Grupper och Ekvivalenta kvadratiska former

Låt $M$ och $N$ vara två $2x2$ matriser med heltalskoefficienter. Då är produkten av matriserna också en $2x2$ matris med heltalskoefficienter.
Om $det(M) = 1$ och $det(N) = 1$ så gäller att $det(MN) = det(M)det(N) = 1 \cdot 1 = 1$.
Dessutom är $M$ inverterbart och $M^{-1}$ har heltalskoefficienter och $det(M^{-1}) = 1$. Det följer att mängden av $2x2$ matriser med heltalskoefficienter och determinant 1 bildar en grupp.

**Definition 5: Den Modulära gruppen**
Den modulära gruppen är gruppen av $2x2$ matriser med heltalselement och determinant 1 och betecknas med Γ.
Den modulära gruppen är inte kommutativ dvs. i allmänhet gäller $MN \neq NM$.

**Exempel 10:**

$$M = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$$

$$N = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$$

$$det(M) = 2 \cdot 2 - 3 \cdot 1 = 4 - 3 = 1$$
$$det(N) = 5 \cdot 1 - 2 \cdot 2 = 5 - 4 = 1$$

$$M \cdot N = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 \cdot 5 + 1 \cdot 2 & 2 \cdot 2 + 1 \cdot 1 \\ 3 \cdot 5 + 2 \cdot 2 & 3 \cdot 2 + 2 \cdot 1 \end{pmatrix} = \begin{pmatrix} 12 & 5 \\ 19 & 8 \end{pmatrix}$$

$$N \cdot M = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 \cdot 2 + 2 \cdot 3 & 5 \cdot 1 + 2 \cdot 2 \\ 2 \cdot 2 + 1 \cdot 3 & 2 \cdot 1 + 1 \cdot 2 \end{pmatrix} = \begin{pmatrix} 16 & 9 \\ 7 & 4 \end{pmatrix}$$

**Definition 6: Ekvivalenta kvadratiska former**
Två kvadratiska former $f(x,y) = ax^2 + bxy + cy^2$ och $g(x,y) = Ax^2 + Bxy + Cy^2$ är *ekvivalenta* om det finns en matris $M = (m_{ij}) \in \Gamma$ så att
$g(x,y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$. Detta betecknas med $f \sim g$ och man säger att $M$ tar $f$ till $g$. Då kan koefficienterna till $g$ uttryckas i termer av $f$ och $M$ som följer:

$$A = am_{11}{}^2 + bm_{11}m_{21} + cm_{21}{}^2 = f(m_{11}, m_{21})$$
$$B = 2am_{11}m_{12} + b(m_{11}m_{22} + m_{12}m_{21}) + 2cm_{21}m_{22}$$
$$C = am_{12}{}^2 + bm_{12}m_{22} + cm_{22}{}^2 = f(m_{12}, m_{22})$$

Betrakta matriserna:

$$F = \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}$$

$$G = \begin{pmatrix} A & \frac{1}{2}B \\ \frac{1}{2}B & C \end{pmatrix}$$

$$X = \begin{pmatrix} x \\ y \end{pmatrix}$$

Då gäller att:
$X^tFX = [f(x,y)]$ och $X^tGX = [g(x,y)]$ där $X^t$ är transponatet till $X = \begin{pmatrix} x \\ y \end{pmatrix}$.
Vi får $g$ genom att beräkna $f$ med $MX$ istället för $X$.
Notera att $(MX)^t = M^tX^t$, därför $(MX)^tF(MX) = X^t(M^tFM)X = [g(x,y)]$.

Koefficientmatrisen $G$ av den kvadratiska formen $g$ kan alltså bestämmas av koefficienterna till $g$ genom att beräkna $G = M^tFM$.

Vi har nu fått en så kallad ekvivalensrelation ur **definition 6**. Kom ihåg att en relation kallas en ekvivalensrelation om den är reflexiv, symmetrisk och transitiv. Vi ska titta lite närmare på de tre egenskaperna nedan.

## 2.3 Relationer och reducerade former

**Sats 9: ~ är en ekvivalensrelation**
Låt $f, g$ och $h$ vara binära kvadratiska former. Då gäller att:
i) $f \sim f$ (reflexiv)
ii) Om $f \sim g$ så $g \sim f$ (symmetrisk)
iii) Om $f \sim g \; och \; g \sim h$ så $f \sim h$ (transitiv)

**Bevis:**

i) $f \sim f$: Låt $M = I$ vara identitetsmatrisen. Då gäller att I ∈ Γ och $I^tFI = F$, vilket medför att $f \sim f$.

ii) Anta att $f \sim g$. Då gäller att $M^tFM = G$, för något M ∈ Γ. Multiplicerar vi $M^tFM = G$ med $(M^{-1})^t$ från vänster och $M^{-1}$ från höger, får vi att $F = (M^{-1})^tGM^{-1}$. Men eftersom Γ är en grupp så är $M^{-1} \in \Gamma$ och därför $g \sim f$.

iii) Anta att $f \sim g$ och $g \sim f$. Då har vi att $G = M^{-1}FM$ och $H = N^{-1}GN$ där $M, N \in \Gamma$. Sätter vi $G = M^{-1}FM \; in \; i \; H = N^{-1}GN$ så får vi att:
$H = N^{-1}(M^{-1}FM)N = (MN)^{-1}F(MN)$.
Eftersom $MN \in \Gamma$ så är $f \sim h$.■

Eftersom relationen $(\sim)$ är en ekvivalensrelation så bildar partitioner av binära kvadratiska former ekvivalensklasser. Det ska vi använda i **sats 10** nedan för återgivning av heltal.

**Sats 10**
Låt $f$ och $g$ vara två ekvivalenta binära kvadratiska former. Då gäller för varje givet heltal $n$ att representationerna för $n$ av $f$ står i bijektiv korrespondens med representationerna för $n$ av $g$. På samma sätt korresponderar propra representationerna för $n$ av $f$ och $g$, vidare är diskriminanten till $f$ och $g$ lika.

**Bevis:**
Första påståendet följer av **sats 8 och definition 6**. För andra påståendet så ska vi visa att $sgd(x, y) = sgd(u, v)$ för nollskilda gitterpunkter $U \; och \; X$ där $U = MX$.
Låt $r = sgd(x, y) \; och \; s = sgd(u, v)$. Eftersom $\frac{1}{r}X$ är en gitterpunkt så medför **sats 8** att $\frac{1}{r}X = M(\frac{1}{r}X)$ är en gitterpunkt. Alltså $r|s$. På samma sätt får vi att $s|r$ som betyder att $r = s$.
Låt nu $d$ vara diskriminanten av $f$ och $D$ vara diskriminanten av $g$. Observera att

$det(F) = -\frac{d}{4}$ och $det(G) = -\frac{D}{4}$.
Då ger $G = M^tFM$ och $det(MN) = det(M)det(N)$ att:
$det(G) = -\frac{D}{4} = det(M^tFM) = det(M^t) \cdot det(F) \cdot det(M) = det(F) = -\frac{d}{4}$.■

Vi har diskuterat *ekvivalenta* former abstrakt hittills. Nu ska vi studera hur man med hjälp av en särskild klass av former, nämligen *reducerade former,* kan avgöra om två former är *ekvivalenta*. Vi ska också introducera en metod för att hitta en *reducerad form* som är ekvivalent med vilken given form som helst.

**Definition 8: Reducerade former**
Låt $f$ vara en binär kvadratisk form med en diskriminant $d$ som ej är en kvadrat. Då kallas $f$ *reducerad* om $-|a| < b \leq |a| < |c|$ $eller$ $0 \leq b \leq |a| = |c|$.

Vi ska nu tillämpa två olika transformationer:
**1)** Låt $f$ vara en given binär kvadratisk form med en diskriminant $d$ som ej är en kvadrat. Då ger **sats 2** att $a \neq 0$ och $c \neq 0$. Om [$|c| < |a|$ eller $|c| = |a|$ och $-|a| \leq b < 0$], ta matrisen $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Vi får att $f$ är ekvivalent med formen $g(x,y) = cx^2 - bxy + ay^2$.
**2)** Om $b$ inte ligger i intervallet $(-|a|, |a|]$, så tar vi $M = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ i $M^tFM = G$.
Nu ser vi från avsnitt 2.4 att:
$A = a, B = 2am + b$ och $C = f(,1) = am^2 + bm + c$.
Låt $m$ vara ett unikt heltal så att $-|a| < B \leq |a|$.
Det kan ge oss en icke reducerad form eftersom $|C| < |A|$ kan inträffa. I så fall räknar vi först med **1)**, annars tar vi **2)**. Dvs. genom att tillämpa båda får vi i slutändan en reducerad form ur ett av de två alternativen. Processen är ändlig och leder till en reducerad form eftersom koefficienten till $x^2$ är avtagande och enligt **1)** är koefficienten strikt avtagande om inte $|a| = |c|$.

**Sats 11**
Låt $b$ vara ett givet icke-kvadratiskt heltal. Då gäller att varje ekvivalensklass av binära kvadratiska former av diskriminant $d$ har minst en reducerad form.

I sista avsnittet av det här arbetet vi ska visa att om $d < 0$ så är den reducerade formen i en given ekvivalensklass unik. Detta gäller dock generellt inte för $d > 0$.

**Exempel 11:**
Hitta en reducerad form ekvivalent med $266x^2 + 216xy + 44y^2$.

**Lösning:**
Eftersom $|c| < |a|$ så använder vi 1); alltså
$266x^2 + 216xy + 44y^2 \sim 44x^2 - 216xy + 266y^2$.

Vi vet att:
$A = a = 44$
$B = 2am + b = 88m - 216$
$C = f(m,1) = am^2 + bm + c$

Nu bestämmer vi det unika heltalet $m$ så att $-|a| < B \leq |a|$. Så:

$$-44 < 88m - 216 \leq 44$$
$$<=>$$
$$-11 < 22m - 54 \leq 11$$
$$<=>$$
$$43 < 22m \leq 65$$

Vi ser att det unika heltalet $m$ som uppfyller kravet ovan är:
$m = 2$, dvs. $43 < 44 \leq 65$.

Vidare ser vi att:
$A = 44$
$B = -40$
$C = 10$

Nu har vi:
**Enligt 2):**
$44x^2 - 216xy + 266y^2 \sim 44x^2 - 40xy + 10y^2$.
**Enligt 1):**
$44x^2 - 40xy + 10y^2 \sim 10x^2 + 40xy + 44y^2$.

Eftersom $40 \notin (-10,10]$ så medför **2)** att:

$$-10 < 20m + 40 \leq 10$$
$$<=>$$
$$-50 < 20m \leq -30$$
$$<=>$$
$$-5 < 2m \leq -3$$

Vi ser att $m = -2$, dvs. $-5 < -4 \leq -3$. Vidare ser vi att:
$A = 10$
$B = 0$
$C = 4$
Dvs. $10x^2 + 40xy + 44y^2 \sim 10x^2 + 4y^2$ som är **enligt 1)** ekvivalent med $4x^2 + 10y^2$, vilken är den reducerade formen.

För att beräkna diskriminanten räcker det att beräkna en av formernas diskriminant, eftersom de är ekvivalenta. Vi beräknar $d$ till den reducerade formen och får:
$d = b^2 - 4ac = 0^2 - 4 \cdot 4 \cdot 10 = -160$

**Sats 12**
Låt $f$ vara en reducerad binär kvadratisk form med diskriminant $d$. Då gäller att om $f$ är *indefinit* så är $0 < |a| \leq \frac{1}{2}\sqrt{d}$. Om $f$ är *positivt definit* så är $0 < a \leq \sqrt{\frac{-d}{3}}$.
I båda fall gäller att antal reducerade former med diskriminant $d$ är ändligt många.

**Bevis:**
Om $a$ och $c$ har samma tecken så gäller att:

$d = b^2 - 4ac = b^2 - 4|ac| \leq a^2 - 4|ac| \leq a^2 - 4a^2 < 0$. Vidare om $d > 0$ så är $ac < 0$.
Därför $d = b^2 - 4ac = b^2 + 4|ac| \geq 4|ac| \geq 4a^2$, som i detta fall ger oss gränsen för $|a|$.
Om $d < 0$ så är $a > 0$ och $c > 0$. Därför:
$d = b^2 - 4ac \leq a^2 - 4ac \leq a^2 - 4a^2 = -3a^2$, som i detta fall ger oss gränsen till $a$.
Vi ser att i vilket fall som helst kan $a$ och $b$ ha ändligt många värden. Då gäller att för varje valda $a$ och $b$ finns det högst ett heltal $c$ sådant att $d = b^2 - 4ac$.■

**Definition 9**
Om $d$ inte är en perfekt kvadrat så kallas antalet ekvivalensklasser av binära kvadratiska former med diskriminant $d$, *klasstalet* av $d$ och betecknas med $H(d)$.

# 3 *Summan av två kvadrater*

I det här avsnittet ska vi bland annat studera vad som krävs för att kunna skriva ett givet heltal $n$ som en summa av två kvadrater, dvs. $n = x^2 + y^2$.
Det finns olika metoder för att lösa en sådan uppgift, men innan vi ger oss in i lösningsmetoden ska vi först introducera några beteckningar.

$N(n) =$ Antal lösningar $s\ (mod\ n)$ till $s^2 \equiv -1(mod\ n)$.
$R(n) =$ Antal ordnade heltalspar $(x, y)$ sådana att $x^2 + y^2 = n$.
$P(n) =$ Antal propra representationer av $n$ av formen $x^2 + y^2$ med $x > 0$ och $y \geq 0$.
$r(n) =$ Antal ordnade heltalspar $(x, y)$ så att $x^2 + y^2 = n$ med $sgd(x, y) = 1$, dvs. antal propra representationer av $n$.

Först konstaterar vi att $f(x, y) = x^2 + y^2$ med $a = 1, b = 0\ och\ c = 1$ har diskriminant $d = b^2 - 4ac = 0^2 - 4 \cdot 1 \cdot 1 = 0 - 4 = -4$.
Vi ska nu lista ut alla reducerade kvadratiska former till $d = -4$. Här ska vi bara fokusera på positivt definita former.
Vi har att $d = -4$. Från **sats 12** får vi att $0 < a \leq \sqrt{\frac{-d}{3}} \Rightarrow 0 < a \leq \sqrt{\frac{4}{3}}$, alltså $a = 1$.
Vidare ger **definition 8** att $b = 0$ eller 1, men $b = 1$ är omöjligt eftersom $b^2 - 4ac = -4$.
Därför $b$ måste vara 0. Vidare får vi att $c = 1$.
Därför är $f(x, y) = x^2 + y^2$ den enda reducerade formen med diskriminanten $d = -4$. Då följer det av **sats 11** att alla positivt definita former med diskriminant $d = -4$ är ekvivalenta.
Alltså; $H(-4) = 1$.

## 3.1 Kongruens och primtal

**Sats 14**
Låt $p$ vara ett primtal. Då gäller att $x^2 \equiv -1(mod\ p)$ har lösningar om och endast om $p = 2$ eller $p \equiv 1(mod\ 4)$.

**Bevis:**
För $p = 2$ har vi att $x = 1$ eftersom $1^2 = 1 \equiv -1\ (mod\ 2)$.
För udda primtal medför **Eulers Kriterium** att $(-1)^{(p-1)/2} = 1$ om och endast om $(p - 1)/2$ är ett jämnt tal, med andra ord om och endast om primtalet $p$ är på formen $p = 4k + 1$, för något heltal $k$.■

**Sats 15**
Om $d|m$, $d > 0$, och om $l$ är en lösning till $f(x) \equiv 0(mod\ m)$, så är $l$ också en lösning till $f(x) \equiv 0\ (mod\ d)$.

**Lemma 1: Hensel's Lemma**
Anta att $f(x)$ är ett polynom med heltalskoefficienter. Om $f(a) \equiv 0(mod\ p^j)$ och $f'(a) \not\equiv 0(mod\ p)$ så finns det en unik restklass $t(mod\ p)$ så att $f(a + tp^j) \equiv 0(mod\ p^{j+1})$.

## 3.2 Representationer av summan av två kvadrater

**Sats 16: Proper representation**
Ett positivt heltal $n$ är en proper representation av summan av två kvadrater om och endast om primtalen i $n$ är alla av typ $4k + 1$, förutom primtalet 2, och $n$ inte är delbart med 4.

**Bevis:**
Enligt **sats 5** och **sats 10** är ett positivt heltal $n$ är propert representerat av $x^2 + y^2$ om och endast om $d = -4$ är en kvadrat $(mod\ 4n)$. Lägg märke till att $-4$ är en kvadrat $(mod\ 8)$ men inte $(mod\ 16)$, därför får $n$ vara delbart med 2 men inte med 4. Om $p$ är ett udda primtal på formen $4k + 1$ så är $-4$ en kvadrat $(mod\ p)$ enligt **sats 14.** Det vill säga om $f(x) = x^2 + 4$ så har $f(x) \equiv 0(mod\ p)$ en lösning $x_0$. Eftersom $f'(x_0) = 2x_0 \not\equiv 0(mod\ p)$, så ger **Hensel's lemma** att lösningen kan lyftas till en unik lösning $(mod\ p^2)$, $(mod\ p^3)$ och så vidare. Därför kan $n$ vara delbart med godtyckliga potenser av primtal av typ $4k + 1$, dvs. $p = 4k + 1$, $p^j$ för $j = 1,2, \dots, n$. Å andra sidan om $p$ är ett primtal av typ $p = 4k + 3$ så ger **sats 14** att $-4$ inte är kvadrat $(mod\ p)$. Så enligt **sats 15** är $-4$ inte en kvadrat $(mod\ 4n)$.■

**Exempel 12:**
Bestäm heltalen $x$ och $y$ så att:

$x^2 + y^2 = 7$

**Lösning:**
Ekvationen saknar lösning, ty 7 inte är på formen $4k + 1$. Det är klart att 7 inte kan skrivas som en summa av två kvadrerade heltal. Samma sak gäller 3,6,8,10,11,12…,.

**Sats 17**
Anta att $n > 0$, och låt $N(n)$ vara antal lösningar till $s^2 \equiv -1\ (mod\ n)$. Då gäller att $r(n) = 4N(n)$ och $R(n) = \sum r(\frac{n}{d^2})$ där summan sträcker sig över alla positiva $d$ som uppfyller $d^2|n$.

**Exempel 13:**
Låt $n = 2$. Bestäm $N(n), r(n)$ och $R(n)$.

**Lösning:**
Först hittar vi heltalslösningar till $s^2 \equiv -1\ (mod\ 2)$, om det finns sådana. Om ekvationen saknar heltalslösningar så är $r(n) = R(n) = 0$. Vi ska testa $s = 0,1$ eftersom det är $(mod\ 2)$. Vi har att:
**$s = 0$**:
$s^2 \equiv -1\ (mod\ 2)$, vi skriver om ekvationen och får:

$s^2 + 1 \equiv 0\ (mod\ 2)$, $s = 0$ ger:
$0^2 + 1 \equiv 0\ (mod 2)$
$1 \not\equiv 0\ (mod 2)$.
Dvs. $s = 0$ är ingen lösning.
**s = 1**:
$s^2 \equiv -1\ (mod\ 2)$
$s^2 + 1 \equiv 0 (mod\ 2)$
$1^2 + 1 = 2 \equiv 0\ (mod\ 2)$.
Ekvationen $s^2 \equiv -1\ (mod\ 2)$ har alltså en heltalslösning, $s = 1$.
Enligt **sats 17:**

$r(2) = 4 \cdot 1 = 4$
$R(2)\ = \sum r(\frac{2}{d^2})$

Vi vet att det enda positiva $d$ så att $d^2|n$ är $d = 1$. Vi sätter in $d = 1$ i $R(2)$ och får:
$R(2)\ = \sum r(\frac{2}{1^2}) = r(2) = 4$

Svar: $N(2) = 1, r(2) = 4\ och\ R(2) = 4$.

Det är inte alltid kongruensekvationen har lösningar, ibland saknas det lösningar för något heltal $n$. I exemplet ovan hade vi $n = 2$ men det skulle kunna vara vilket stort positivt $n$ som helst. Vi kommer att introducera en ny sats som underlättar beräkningen för stora värden på $n$. Det ska vi göra i **sats 19** i slutet av detta avsnitt.

Ta för enkelhets skull $n = 15$. Då är $r(15) = 0, R(15) = 0\ och\ N(15) = 0$, ty kongruensekvationen saknar heltalslösningar. Men istället för att testa alla $s = 0{,}1 \ldots 14$, beräknar vi $x^2 + y^2 = 15$. Vi ser att det inte finns heltal $x, y$ som uppfyller ekvationen, därför saknar den lösningar och vidare är $r(15) = 0\ och\ R(15) = 0$.

Tillbaka till **exempel 13,** $r(2) = 4$ betyder att vi har 4 stycken ordnade par med $sgd(x, y) = 1$. Om uppgiften hade krävt att lista ut alla sådana par då är det enkelt för små $n$ men mycket svårare för stora $n$. I fallet $x^2 + y^2 = 2$ ser vi direkt att $x = \pm 1\ och\ y = \pm 1$, därför $(1{,}1), (-1, -1), (-1{,}1), (1, -1)$ är de 4 olika ordnade paren. Samma fyra par gäller R(2), i just detta exempel.

**Sats 18**
Låt $n$ vara ett positivt heltal så att $x^2 + y^2 = n$ och att primtalsfaktoriseringen av talet $n$ innehåller primtalsfaktorn $p$, där $p \equiv 3\ (mod\ 4)$. Då gäller att:
$(i)$ $p|x$ och $p|y$
$(ii)$ $p$ måste förekomma som en jämn potens i primtalsfaktoriseringen av n

**Bevis:**
$(i)$ Anta att $p \nmid x$. Då finns det ett heltal $r$ sådant att $ra \equiv 1\ (mod\ p)$. Vi multiplicerar kongruensekvationen $x^2 + y^2 \equiv 0\ (mod\ p)$ med $r^2$och får

$$(ry)^2 = r^2y^2 \equiv -r^2x^2 \equiv -1\ (mod\ p).$$

Vilket betyder att $-1$ är en kvadratisk rest $(mod\ p)$. Men enligt **sats 14** är det en motsägelse. Därför $p|x$ och av symmetrin även $p|y$.
$(ii)$ Eftersom $p|\ x\ och\ p\ |\ y$ samt $n\ =\ x^2+\ y^2$, medför det att $p^2\ |\ n$. Genom att dividera ekvationen $n\ =\ x^2\ +y^2$ med $p^2$ får vi ekvationen $\frac{n}{p^2}=(\frac{x}{p})^2+(\frac{y}{p})^2$, vilket innebär att talet $t=\ \frac{n}{p^2}$, är en summa av två kvadrater. Enligt argumentet ovan, om $p\ |\ t$ så även $p^2\ |\ t$. Om vi fortsätter med processen på samma sätt så ser vi att $n$ måste vara delbart med en jämn potens av $p$.■

**Lemma 2:**
Om två heltal $u$ och $v$ är summor av två kvadrater så är deras produkt också en summa av två kvadrater. D.v.s. om:
$u={x_1}^2+{y_1}^2$
$v={x_2}^2+{y_2}^2$
Så är:
$uv=\big(({x_1}^2+{y_1}^2)(\ {x_2}^2+{y_2}^2)\big)=((x_1x_2+y_1y_2)^2+(x_1y_2-x_2y_1)^2)$

**Exempel 14:**
Hitta samtliga heltalslösningar $x$ och $y$ så att $x^2+y^2=1989$.

**Lösning:**
Först faktoriserar vi $n$:
$n=1980=3^2\cdot13\cdot17$
$3^2$ Ok! ty har jämn exponent samt $3\equiv3\ (mod\ 4)$.
Eftersom 13 och 17 har exponent 1, så måste $13\not\equiv3\ (mod\ 4)\ och\ 17\not\equiv3\ (mod\ 4)$ annars saknar ekvationen lösningar. Men $13\equiv1\ (mod\ 4)\ och\ 17\equiv1\ (mod\ 4)$ Ok!
Vi vet att 13 kan skrivas som:
$13=9+4=(3^2+2^2)$
På samma sätt 17:
$17=16+1=(4^2+1^2)$
Nu har vi att:
$x_1=3,y_1=2,x_2=4,y_2=1$

Enligt **lemma 2,** får vi:

$(x_1+x_2)^2(y_1+y_2)^2=((x_1x_2+y_1y_2)^2+(x_1y_2-x_2y_1)^2)=$
$((3\cdot4+2\cdot1)^2+(3\cdot1-2\cdot4)^2)=>$
$1989=3^2(14^2+(-5)^2)=(3\cdot14)^2+(3\cdot(-5))^2=42^2+(-15)^2$

Nu byter vi plats på (+) och (-) tecknen i respektive parantes och får:

$((x_1+x_2)^2(y_1+y_2)^2)=((x_1x_2-y_1y_2)^2+(x_1y_2+x_2y_1)^2)=$
$((3\cdot4-2\cdot1)^2+(3\cdot1+2\cdot4)^2)=>$
$1989=3^2(10^2+11^2)=(3\cdot10)^2+(3\cdot11)^2=30^2+33^2$

Eftersom $x$ och $y$ tas i kvadrat så kan de negeras i ekvationen. Alltså får vi totalt 16 lösningar:

$x=\pm42,\ \ y=\pm15$
$x=\pm30,\ \ y=\pm33$

$x = \pm 15,\ \ y = \pm 42$
$x = \pm 33,\ \ y = \pm 30$
Vi ska nu bestämma $r(1989)$ och $R(1989)$.
Enligt **sats 16,** $r(1989) = 0$.
Enligt **sats 17,**
$R(n) = \sum r(\frac{n}{d^2})$ , där $d = 3$. Vi sätter in $n$ och $d$ och får att:
$R(1989) = \sum r\left(\frac{1989}{3^2}\right) = \sum r(221)$.
Från **sats 17** vet vi att:
$r(221) = 4N(221)$, där $N(221)$ är antal lösningar till $s^2 \equiv -1\ (mod\ 221)$.
Vi löser kongruensekvationen och får 4 lösningar, nämligen:
$x = 21, x = 47, x = 174, x = 200$
Alltså får vi att:
$r(221) = 4N(221) = 4 \cdot 4 = 16$
Dvs. $R(1989) = \sum r\left(\frac{1989}{3^2}\right) = \sum r(221) = 16$. Vilket stämmer överens med antal lösningar vi fick ovan. Så:
$r(1989) = 0$
$N(221) = 4$
$R(1989) = 16$
Vi vet att $R(1989) = 16$, som visar att ekvationen $x^2 + y^2 = 1989$ har endast 16 lösningar $(x, y) \in \mathbb{Z}$.

Vi har sett i **sats 17** och **exempel 14** hur $r(n)\ och\ R(n)$ kan bestämmas. Vi har också sett att det kan bli besvärligare för stora heltal $n$ att beräkna $r(n)\ och\ R(n)$. Vi ska nu introducera en ny metod som underlättar dessa beräkningar.

**Sats 19**
Låt $n$ vara ett positivt heltal med $n = 2^\alpha \prod_p p^\beta \prod_q q^\gamma$ där $p = 4k + 1$ är primtal som delar $n$ och $q = 4k + 3$ primtal som delar $n$. Om $\alpha = 0$ eller 1 och alla $\gamma = 0$, så gäller att $r(n) = 2^{t+2}$ där $t$ är antalet primtal av formen $p = 4k + 1$ som delar $n$. I annat fall $r(n) = 0$. Om alla $\gamma$ är jämna så gäller att $R(n) = 4\prod_p(\beta + 1)$. I annat fall $R(n) = 0$.

**Exempel 15:**
Bestäm $r(n)$ och $R(n)$ om $n = 89082$.

**Lösning:**
Först primfaktoriserar vi $n$:
$n = 89082 = 2 \cdot 9 \cdot 49 \cdot 101 = 2 \cdot 3^2 \cdot 7^2 \cdot 101.$
Enligt **Sats 19,** $89082 = 2^\alpha \prod_p p^\beta \prod_q q^\gamma$.
Vi ser direkt att $p = 101, q_1 = 3\ och\ q_2 = 7$, som visar att $\alpha = 1, \beta = 1, \gamma_1 = \gamma_2 = 2$.
$p = 101$, ty
$101 \equiv 1\ (mod\ 4)$
På samma sätt:
$q_1 = 3 \equiv 3\ (mod\ 4)$
$q_2 = 7 \equiv 3\ (mod\ 4)$
Nu:
$n = 2^1 \cdot 101 \cdot 3^2 \cdot 7^2$
Vidare är enligt **sats 19,** $r(89082) = 0$, ty $\gamma_1 = \gamma_2 = 2 \neq 0$.
Eftersom $\gamma_1\ och\ \gamma_2$ är jämna så får vi enligt **sats 19** att:

$R(n) = 4\prod_p(\beta + 1)$, där $p$ löper genom alla primtal av formen $p = 4k + 1$ som delar $n$. $R(89082) = 4 \cdot (1 + 1) = 4 \cdot 2 = 8$, ty 101 är enda primtal på formen $p = 4k + 1$ som delar 89082.

Om vi skulle vara intresserade av de 8 ordnade heltalsparen, så kan vi bestämma dem som i **exempel 14** vilket ger:

$x = \pm 231, y = \pm 189$
$x = \pm 189, y = \pm 231$

Kombinerar vi alla möjliga par $(x, y)$, får vi 8 stycken.

Som vi ser leder satserna till samma resultat fast någon sats är enklare att räkna med jämfört med den andra. Exempelvis i **exempel 15** ovan var det enklare att bestämma $r(n)$ enligt **sats 19** istället för **sats 17,** så undviker vi att räkna kongruensekvationen för $s = 0, \dots, 89081$ vilken saknar heltalslösningar.

# *4 Positivt definita binära kvadratiska former*

Hittills har vi introducerat olika detaljer om definita och indefinita former. Nu ska vi fokusera på positivt definita kvadratiska former $f(x, y) = ax^2 + bxy + cy^2$. Som vi vet är varje form $f(x, y) = ax^2 + bxy + cy^2$ ekvivalent med en reducerad form. I detta avsnitt ska vi visa att två olika reducerade former inte är ekvivalenta.

## 4.1 Representationer av reducerade positivt definita former

**Lemma 3**
Låt $f(x, y) = ax^2 + bxy + cy^2$ vara en reducerad positivt definit form. Låt $x$,$y$ vara ett heltalspar. Om $sgd(x, y) = 1$ och $f(x, y) \leq c$ så är $f(x, y) = a$ eller $c$. Då är punkten $(x, y)$ en av punkterna $\pm(1,0), \pm(0,1), \pm(1, -1)$. I så fall är antalet propra representationer av $a$:

$$\begin{cases} 2 & om \quad a < c \\ 4 & om \quad 0 \leq b < a = c \\ 6 & om \quad a = b = c \end{cases}$$

Vi utelämnar beviset.

**Sats 20**
Låt $f(x, y) = ax^2 + bxy + cy^2$ och $g(x, y) = Ax^2 + Bxy + Cy^2$ vara två reducerade positivt definita kvadratiska former. Då gäller att om $f \sim g$ så är $f = g$.

**Bevis:**
Anta $f \sim g$. Enligt **lemma 3,** är $a$ det minsta positiva tal som kan representeras propert av $f$. På samma sätt är $A$ till $g$. Vidare medför **Sats 10** $att\ A = a$.
Låt först $a < c$. Då ger **lemma 3** exakt två propra representationer av $a$ med $f$. Då följer det av **sats 8** att det finns exakt två propra presentationer av $a$ med $g$. Vidare medför **lemma 3** att $C > a$.
Nu **lemma 3**, $c$ är det minsta proper representerade tal i $f$ som är större än $a$. På samma sätt är $C$ det minsta i $g$. Vidare medför **sats 3** att $c = C$.

För att visa att $b = B$, betraktar vi matriserna $M \in \Gamma$ som tar $f$ till $g$.

Eftersom $det(M) = m_{11}m_{22} - m_{21}m_{12} = 1$ så är $sgd(m_{11}, m_{21}) = 1$. Då medför $A = am_{11}{}^2 + bm_{11}m_{21} + cm_{21}{}^2 = f(m_{11}, m_{21})$ (**i definition 6**) att $f(m_{11}, m_{21}) = a$ är en proper representation till $a$. Nu följer det av **lemma 3** att första kolumn i $M$ är $\pm\binom{1}{0}$.
På samma sätt får vi att $sgd(m_{11}, m_{21}) = 1$. Vidare medför $C = am_{12}{}^2 + bm_{12}m_{22} + cm_{22}{}^2 = f(m_{12}, m_{22})$ (**i definition 6**) att $f(m_{12}, m_{22}) = c$ är en proper representation till $c$. Enligt **lemma 3,** andra kolumnen i $M$ är $\pm\binom{0}{1}$ eller $\binom{-1}{1}$. Nu har vi två möjligheter till $M$, nämligen $\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ och $\pm\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}$.

I fallet $B = 2am_{11}m_{12} + b(m_{11}m_{22} + m_{12}m_{21}) + 2cm_{21}m_{22}$ får vi att $B = -2a + b$ som är omöjligt eftersom $b$ och $B$ ska ligga i intervallet $(-a, a]$.
Dvs. vi har bara $\pm I$ (identitetsmatris) kvar, vilken medför att om $M = \pm I$ så är $f = g$.

Betrakta nu fallet där $a = c$. Då ger **lemma 3** att antal propra representationer till $a$ i $f$ är minst 4. Enligt **Sats 10,** samma sak gäller $g$. Vidare, enligt **lemma 3** gäller att $C = a = c$. Enligt **definition 8,** $0 \le b \le a = c$ $och$ $0 \le B \le A = C = a$. Vilket innebär att om $b^2 - 4ac = B^2 - 4AC$ så är $b = B$ och därför $f = g$. ■

## 4.2 Automorfer

**Definition 10**
Låt $f$ vara en positivt definit binär kvadratisk form. En matris $M \in \Gamma$ kallas en *automorf* till $f$ om $M$ tar $f$ till sig själv, det vill säga om $f(m_{11}x + m_{12}y, m_{21}x + m_{22}y) = f(x, y)$.

Antal automorfer till $f$ betecknas med $w(f)$.

**Exempel 16:**
Betrakta formen $f(x, y) = ax^2 + bxy + by^2$ med $a = b = c = 1$ och diskriminant $d$.
Vi har att:

$f(x, y) = x^2 + xy + y^2$
$d = b^2 - 4ac = 1^2 - 4 \cdot 1 \cdot 1 = 1 - 4 = -3$
$a > 0, d < 0 \Rightarrow f$ är positivt definit OK!

Låt $M = \begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix}$. Vi beräkna determinanten till $M$ och får:

$det(M) = (-1)(0) - (1)(-1) = 1$, $M \in \Gamma$ OK!

$$\begin{aligned} f(m_{11}x + m_{12}y, m_{21}x + m_{22}y) = f(-x - y, x) &= (-x - y)^2 + (-x - y)(x) + x^2 \\ &= x^2 + 2xy + y^2 - x^2 - xy + x^2 \\ &= x^2 + xy + y^2 \end{aligned}$$

Alltså $f(m_{11}x + m_{12}y, m_{21}x + m_{22}y) = f(x, y)$. Därför är $M$ automorf till $f(x, y) = x^2 + xy + y^2$.

**Obs**: $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ och $-\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ är automorfer till *alla* $f$.

**Sats 21**
Låt $f$ och $g$ vara ekvivalenta positivt definita binära kvadratiska former. Då gäller att $w(f) = w(g)$ med exakt $w(f)$ matriser $\in \Gamma$ som tar $f$ till $g$ och $w(f)$ matriser $\in \Gamma$ som tar $g$ till $f$. Möjliga värden på $w(f)$ är 2,4 och 6. Om $f$ är en reducerad form så gäller att:

$w(f) = 4\ om\ a = c\ och\ b = 0$
$w(f) = 6\ om\ a = b = c$
$w(f) = 2\ för\ övrigt$

Vi utelämnar beviset.

Vi ska nu utvidga informationen från föregående avsnitt samt introducera nya beteckningar som leder oss till ännu en sats som är den sista i detta arbete.

Låt $R_f(n)$ vara antalet representationer av $n$ med formen $f$, och låt $r_f(n)$ vara antal propra representationer bland dem.
Låt $H_f(n)$ vara antalet heltal $t$ som uppfyller $t$ där $0 \leq t < 2n$ och $t^2 \equiv d(mod\ 4n)$ och dessutom har egenskapen att om $t^2 = d + 4nk$ så är den kvadratiska formen $nx^2 + txy + ky^2$ ekvivalent med $f$.

**Sats 22**
Låt $f$ vara en positivt definit binär kvadratisk form med diskriminant $d < 0$.
Då gäller för varje positivt heltal $n$ att:
$r_f(n) = w(f)H_f(n)$
och
$R_f(n) = \sum_{m^2|n} r_f\left(\frac{n}{m^2}\right)$, där $m$ löper genom alla positiva heltal som uppfyller $m^2|n$.

Observera att om vi tar $f(x, y) = x^2 + y^2$ i **sats 22** så ser vi att **sats 17** är ett specialfall av **sats 22.** Vi ska visa det med hjälp av resonemanget nedan.

Betrakta formen $f(x, y) = x^2 + y^2$.

Vi konstaterar att diskriminanten av $f$ är $d = b^2 - 4ac = -4$.
Vi vet från **sats 17** att $r(n) = 4N(n)$. Enligt **sats 22** har vi att $r_f(n) = w(f)H_f(n)$. Vi vet också att $r(n) = r_f(n)$. Eftersom $a = c = 1\ och\ b = 0$, så får vi enligt **sats 21** att $w(f) = 4$.
Nu har vi att $r_f(n) = 4H_f(n)$ och $r(n) = 4N(n)$. För att $r_f(n) = 4H_f(n)$ och $r(n) = 4N(n)$ ska gälla så måste $H_f(n)$ vara lika med $N(n)$.
Vi vet att:
$N(n)$ är antal lösningar till $s^2 \equiv -1\ (mod\ n)$.
och
$H_f(n)$ är antal heltal $t$ där $0 \leq t < 2n$ så att $t^2 \equiv d(mod\ 4n)$. (Här utnyttjar vi att $H(-4) = 1$.).
Det återstår att se om, $s^2 \equiv -1\ (mod\ n)$ och $t^2 \equiv d(mod\ 4n)$ är samma.
Från $t^2 \equiv d(mod\ 4n)$ ser vi att $4|t^2$, som medför att $2|t$.
Nu låter vi $t = 2s$, som medför att $0 \leq s \leq n$. Vi sätter $t = 2s$ in i $t^2 \equiv -4\ (mod\ 4n)$ och får:

$(2s)^2 \equiv -4\ (mod\ 4n)$
$4s^2 \equiv -4\ (mod\ 4n).$

Vi ser att både HL och VL är delbara med 4. Vi dividerar överallt med 4 och får att:

$(2s)^2 \equiv -4\ (mod\ 4n)$
$4s^2 \equiv -4\ (mod\ 4n)$
$s^2 \equiv -1\ (mod\ n).$

Dvs. $H_f(n) = N(n)$. Vidare får vi att $r_f(n) = w(f)H_f(n) = r(n) = 4N(n)$.■

**Exempel 17:**
Bestäm $r_f(n)$ och $R_f(n)$ om $f(x,y) = x^2 + y^2$ och $n = 2$.

**Lösning:**
Enligt **sats 21** om $a = c\ och\ b = 0$ så $w(f) = 4$.
Vi beräknar $H_f(n)$ och får att:
$d = b^2 - 4ac = 0^2 - 4 \cdot 1 \cdot 1 = -4$
$t^2 \equiv -4\ (mod\ 8)$
Vi testar $t = 0,1,2,3,4,5,6,7$ och får att $t = 2$ och $t = 6$ löser kongruensekvationen. Men vi vet att $0 \leq t < 4$, som ger oss att antal $t$ i intervallet är 1. Därför är $H_f(2) = 1$.
Vi har alltså att:

$r_f(2) = w(f)H_f(2) = 4 \cdot 1 = 4$

Vi vet att möjliga värden på $m$ så att $m^2|n$ är $m = 1$. Därför får vi att:

$R_f(2) = \sum_{m^2|n} r_f\left(\frac{2}{1^2}\right) = r_f(2) = 4.$

**Exempel 18:**
Visa att varje positivt definit kvadratisk form med diskriminant $-3$ är ekvivalent med $f(x,y) = x^2 + xy + y^2$. Visa att ett givet positivt heltal $n$ är propert representerat av $f$ om och endast om $n$ är av formen $n = 3^\alpha \prod p^\beta$, där $\alpha = 0\ eller\ 1$ och alla primtal $p$ är av formen $3k + 1$.

**Lösning:**
Vi vet från **sats 12** att om $f(x,y) = ax^2 + bxy + cy^2$ är en reducerad positivt definit binär kvadratisk form med diskriminant $d = -3$, så är:

$$0 < a \leq \sqrt{\frac{-d}{3}}$$

$$0 < a \leq \sqrt{\frac{-(-3)}{3}}$$

$$0 < a \leq \sqrt{\frac{3}{3}}$$
$$0 < a \leq \sqrt{1}.$$

Vilket medför att $a = 1$. Enligt **definition 8**, och eftersom $c$ måste ha samma tecken som $a$ **(enligt Sats 3)**, så måste nu $-1 < b \leq 1 < c$ eller $0 \leq b \leq 1 = c$. Speciellt är $b = 0$ eller $b = 1$, så $-3 = d = b^2 - 4ac \leq 1 - 4ac$, dvs. $4c \leq 4$, dvs. $c \leq 1$. Alltså måste $c = 1$. Nu följer ur $-3 = b^2 - 4ac$ att alternativet $b = 0$ ej kan gälla, dvs. vi måste ha $b = 1$. Alltså: $a = b = c = 1$.

Vi vet att alla heltal som *propert representeras* av en binär kvadratisk form $f$, *propert representeras* också av den ekvivalenta formen till $f$. Alltså: Varje positivt heltal $n$ som kan propert representeras av någon kvadratisk form med diskriminant -3, kan även propert representeras av formen $x^2 + xy + y^2$. Det följer nu från **sats 5** att detta är möjligt om och endast om kongruensekvationen $x^2 \equiv -3 \ (mod\ 4n)$ har en lösning.

Låt oss lösa kongruensekvationen $x^2 \equiv -3 \ (mod\ 8)$, där $n = 2$.
Fört skriver vi om ekvationen som:
$x^2 + 3 \equiv 0 \ (mod\ 8)$.
Nu testar vi, $x = 1,2..,7$ och får:

$$\begin{aligned}
x = 1: &\quad 1 + 3 = 4 \not\equiv 0 \ (mod\ 8)\\
x = 2: &\quad 4 + 3 = 7 \not\equiv 0 \ (mod\ 8)\\
x = 3: &\quad 9 + 3 = 12 \not\equiv 0 \ (mod\ 8)\\
x = 4: &\quad 16 + 3 = 19 \not\equiv 0 \ (mod\ 8)\\
x = 5: &\quad 25 + 3 = 28 \not\equiv 0 \ (mod\ 8)\\
x = 6: &\quad 36 + 3 = 39 \not\equiv 0 \ (mod\ 8)\\
x = 7: &\quad 49 + 3 = 42 \not\equiv 0 \ (mod\ 8)
\end{aligned}$$

Dvs. kongruensekvationen saknar lösning. Alltså: Om vår kongruensekvation ska ha någon lösning så måste $n$ vara udda. I detta fall ser vi att $x^2 \equiv -3 \ (mod\ 4n)$ har lösningar om och endast om $x^2 \equiv -3 \ (mod\ n)$ har lösningar.

Låt oss nu lösa $x^2 \equiv -3 \ (mod\ 9)$, där $n = 9$.
Vi löser ekvationen på samma sätt som ovan och får:

$$\begin{aligned}
x = 1: &\quad 1 + 3 = 4 \not\equiv 0 \ (mod\ 9)\\
x = 2: &\quad 4 + 3 = 7 \not\equiv 0 \ (mod\ 9)\\
x = 3: &\quad 9 + 3 = 12 \not\equiv 0 \ (mod\ 9)\\
x = 4: &\quad 16 + 3 = 19 \not\equiv 0 \ (mod\ 9)\\
x = 5: &\quad 25 + 3 = 28 \not\equiv 0 \ (mod\ 9)\\
x = 6: &\quad 36 + 3 = 39 \not\equiv 0 \ (mod\ 9)\\
x = 7: &\quad 49 + 3 = 42 \not\equiv 0 \ (mod\ 9)\\
x = 8: &\quad 64 + 3 = 67 \not\equiv 0 \ (mod\ 9)
\end{aligned}$$

Vi ser att denna ekvation också saknar lösningar. Alltså kan primtalet 3 dela $n$ högst en gång ifall vår kongruensekvation ska ha en lösning. Med andra ord måste $\alpha = 0$ eller 1 i primtalsfaktoriseringen $n = 3^{\alpha} \prod p^{\beta}$.

Betrakta nu $n = 3^{\alpha} \prod {p_j}^{\alpha_j}$, där $p_j$ är ett primtal med egenskapen $p_j \geq 5$. Nu har vi enligt **Hensel's lemma** att kongruensekvationen $x^2 \equiv -3 \ (mod \ {p_j}^{\alpha_j})$ har lösningar om och endast om ekvationen $x^2 \equiv -3 \ (mod \ p_j)$ har lösningar, där $p_j$ är primtal sådant att $p_j \geq 5$.
Enligt **sats 7** får vi:

Enligt **(ii):**

$$\left(\frac{-3}{p_j}\right) = \left(\frac{-1}{p_j}\right) \cdot \left(\frac{3}{p_j}\right)$$

Enligt **(vii):**

$$\left(\frac{-3}{p_j}\right) = (-1)^{(p_j-1)/2} \cdot \left(\frac{3}{p_j}\right)$$

Enligt **(v):**

$$\left(\frac{-3}{p_j}\right) = (-1)^{(p_j-1)/2} \cdot \left(\frac{p_j}{3}\right) \cdot (-1)^{(p_j-1)/2}$$

Vidare får vi att:

$$\left(\frac{-3}{p_j}\right) = (1)^{(p_j-1)} \cdot \left(\frac{p_j}{3}\right)$$

Vi vet enligt **definition 4** och **sats 7** att ekvationen $x^2 \equiv -3 \ (mod \ p_j)$ har lösningar om och endast om $p_j \equiv 1 \ (mod \ 3)$, där $p_j \geq 5$.
Alltså ekvationen $x^2 \equiv -3 \ (mod \ 4n)$ har lösningar om och endast om $n$ är av formen $n = 3^{\alpha} \prod p^{\beta}$, där $\alpha = 0 \ eller \ 1$ och alla primtal $p$ är av formen $3k + 1$. Alltså gäller att heltalet $n$ är *propert representerad* av $f$ om och endast om det är av formen $n = 3^{\alpha} \prod p^{\beta}$.■

**Exempel 19:**
Bestäm samtliga primtal som kan representeras av formen $f(x, y) = x^2 + 7y^2$.

**Lösning:**
Först bestämmer vi diskriminanten till $f$. Vi ser att $b = 0, a = 1, c = 7$. Vidare får vi att:
$d = b^2 - 4ac = 0^2 - 4 \cdot 1 \cdot 7 = 0 - 28 = -28$.
Nu ska vi hitta samtliga primitiva reducerade former med diskriminant $-28$. Vi vet från **sats 12** att sådana former måste ha:
$28 = 4ac - b^2$, som visar att b måste vara ett jämnt tal. Vidare vet vi att**:**

$$|b| \leq a \leq \sqrt{\frac{-d}{3}}$$

$$|b| \leq a \leq \sqrt{\frac{28}{3}}$$

Dvs, $|b| < a \leq 3$. Vi konstaterar att $|b| \neq 2$, annars får vi att $a \geq 2$ vilket medför att $28 = 4ac - 4 => 32 = 4ac$. Vidare ser vi att 2 delar både $a$ och $c$, som medför att $a, b, c$ inte är primitiva. Alltså, $f$ är den enda reducerade formen med diskriminant -28.
Vi ser direkt att första tre primtalen inte representeras av f, dvs. primtalen $2,3 \ och \ 5$. Däremot representeras 7 av $f$. Alltså; vi ska bestämma samtliga udda primtalen $p > 7$ som kan representeras av $f$.
Enligt **Legendresymbolen** och **sats 7,** $p$ kan representeras av $f$ om och endast om:

$$\left(\frac{d}{p}\right) = 1$$

Vi konstaterar att $-28 = -1 \cdot 4 \cdot 7 = -1 \cdot 2^2 \cdot 7$. Vidare får vi att:

$$\left(\frac{-28}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right)^2 \cdot \left(\frac{7}{p}\right)$$

$$\left(\frac{-28}{p}\right) = (-1)^{(p-1)/2} \cdot \left(\frac{p}{7}\right) \cdot (-1)^{((p-1)/2)((7-1)/2)}$$

För att $1 = \left(\frac{-28}{p}\right) = (-1)^{(p-1)/2} \cdot \left(\frac{p}{7}\right) \cdot (-1)^{((p-1)/2)((7-1)/2)} = \left(\frac{p}{7}\right)$ ska gälla så måste $p$ vara en kvadrat $(mod\ 7)$. Vidare ser vi att $1,2,4$ är de kvadratiska rester $(mod\ 7)$, vilket medför att $f$ representerar ett udda primtal $p$ om och endast om $p = 7\ eller\ p \equiv 1,2,4\ mod\ (7)$.■

# *5 Referenslista:*

[1] Ivan Niven Herbert S. Zuckerman Hugh L. Montgomery. An Introduction to the Theory of Numbers, 5th Edition, 1991.

[2] SHEPHERD, RICK L., M.A. Binary Quadratic Forms and Genus Theory, 2013.

[3] Elementär talteori. Lars-Åke Lindahl, 2012.

[4] Josh Kaplan, Binary Quadratic Forms, Genus Theory.2014.

[5] John Stillwell, Numbers and Geometry.(1997).

[6] http://mathonline.wikidot.com/legendre-symbol-rules-for-1-p-and-2-p.

[7] http://mathonline.wikidot.com/legendre-symbols.

[8] http://mathonline.wikidot.com/euler-s-criterion.

[9] http://mathonline.wikidot.com/additional-examples-of-evaluating-legendre-symbols.

[10] http://dixon.hh.se/getc/LinSys/KvadratiskaFormer.pdf.