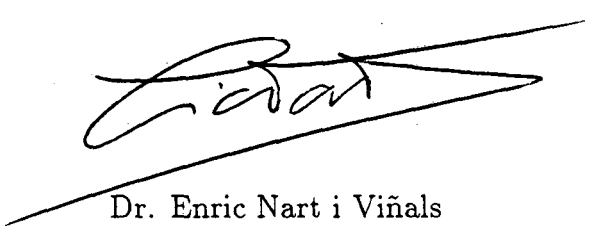
Reducció dels torcements de corbes el·líptiques sobre cossos de nombres

Salvador Comalada i Clara

Memòria presentada al Departament de Matemàtiques de la Universitat Autònoma de Barcelona , per optar al grau de Doctor en Matemàtiques , realitzada sota la direcció del Dr. Enric Nart .

Bellaterra , abril de 1991 .

CERTIFICO que la present Memòria ha estat realitzada per en Salvador Comalada i Clara en el Departament de Matemàtiques de la Universitat Autònoma de Barcelona , sota la meva direcció.



Dr. Enric Nart i Viñals
Departament de Matemàtiques
U.A.B.

Bellaterra , abril de 1991 .

ÍNDEX

INTRODUCCIÓ.

Aquest treball es centra essencialment en l'estudi de la reducció de corbes el·líptiques sobre un cos de nombres K. Aquesta línia de investigació, l'objectiu de la qual és la determinació (mòdul isogènia) de totes les corbes el·líptiques amb conductor prefixat sobre K, fou iniciada fa uns 30 anys, per a contrastar la conjectura de Shimura-Taniyama-Weil a $\mathbb{Q}$. Aquesta important conjectura analítico-modular, enunciada ja l'any 1955 per Taniyama i precisada més tard per Shimura, sosté que tota corba el·líptica E definida sobre $\mathbb{Q}$ és una corba de Weil, o modular, és a dir, existeix un morfisme no-constant $\mathbb{Q}$-racional: $X_0(N) \longrightarrow E$, on N és el conductor de E i $X_0(N)$ és la corba modular respecte del subgrup $\Gamma_0(N) \leq SL_2(\mathbb{Z})$.

Aquesta conjectura implicaria, a més, que les classes d'isogènia de corbes el·líptiques sobre $\mathbb{Q}$ amb conductor N fixat, estarien en correspondència bijectiva amb les formes modulars parabòliques de pes 2 respecte de $\Gamma_0(N)$ que són vectors propis de l'àlgebra de Hecke amb valors propis racionals. Aquesta bijecció tindria la propietat que la transformada de Mellin inversa de la sèrie L de cada corba coincidiria amb la forma modular corresponent. (Per una formulació més precisa de la conjectura, vegi's, per exemple, [Ta1], [Sil2], [Hu]).

La conjectura de Sh-T-W ha estat provada per a corbes amb multiplicació complexa i verificada numèricament -és a dir, comprovant que els dos conjunts esmentats tenen el mateix cardinal- per a corbes amb conductor N petit (vegi's [Og1], [Og2]). És de remarcar que, gràcies a una recent i valuosa aportació de Ribet (cf. [Fre]), es té que la conjectura de Sh-T-W implica la conjectura de Fermat.

Com a conseqüència dels treballs de Weil ([We]) i Jacquet-Langlands ([Ja-La]) que generalitzen als cossos globals la teoria clàssica de Hecke sobre les transformades de Mellin de les sèries de Dirichlet, es formulà una conjectura generalitzada de Sh-T-W, el plantejament de la qual fuig de l'àmbit d'aquest treball. Cal fer notar, però, que aquesta conjectura es troba encara en un estadi incipient en quant a contrastació ([El-Gru-Me], [Krä]).

El problema de la determinació de les corbes el·líptiques sobre un cos de nombres K amb conductor prefixat, es pot enfocar des del punt de vista modular, és a dir, caracteritzant els invariants j d'aquestes corbes. En cada cas, per un teorema de Šafarevič, n'hi haurà un nombre finit. Donat un sistema complet de corbes representants d'aquests j, s'obtenen totes les altres (mòdul isomorfisme) mitjançant torcements d'aquestes (quadràtics, si $j \neq 0, 1728$).

En el nostre treball seguirem aquest plantejament modular i, per això, iniciem la Memòria fent un estudi complet, en el Capítol I, de l'acció dels torcements quadràtics sobre el tipus de reducció de la fibra especial del model v-regular, v-minimal d'una corba el·líptica $E|K$, per a cada valoració discreta v de K. De fet, tota la dificultat per a explicitar aquesta acció es concentra en el cas de $v|2$ i de

torçar per un caràcter χ ramificat a v. Els resultats obtinguts vénen recollits en els teoremes 1.1, 1.2, 1.3 i el corol·lari 1.3, la demostració dels quals es basa en una elecció d'un model de Weierstraß convenient per al torcement E^χ, per tal d'aplicar-li de manera cómoda l'algorisme de Tate (cf. [Ta2]). Així mateix, aquests càlculs ens permeten trobar la relació entre els discriminants minimals de E i E^χ. Aquesta relació ja havia estat explicitada en alguns casos per Silverman [Sil1] i Stevens [Ste], suposant sempre χ no-ramificat sobre els primers de reducció additiva de E.

Utilitzant la relació entre els discriminants minimals, podem donar la relació entre els conductors geomètrics de E i E^χ, una vegada coneixem el nombre de components irreductibles de la fibra especial del model v-regular, v-minimal de E^χ. Aquest nombre és complicat de calcular quan $\mathrm{tip}(E^\chi) = \mathrm{I}_\nu^*$. A la seva computació dediquem la darrera secció del capítol.

En el Capítol II de la Memòria abordem el problema de la caracterització modular de les corbes el·líptiques sobre K amb bona reducció fora d'un conjunt S finit de primers. Per això, considerem prèviament, en la secció 1, el problema local, ja plantejat per Serre i Tate [Se-Ta], que consisteix en la descripció del conjunt $J(v)$, on:

$$J(v) = \{j \in K; \exists \text{ una c.e. } E|K \text{ amb } j(E) = j \text{ i bona reducció a } v\}.$$

Com ja remarcaren Serre i Tate, la dificultat en la descripció de $J(v)$ es situa en els casos $v|6$ [Se-Ta, p. 509].

En els teoremes 2.1, 2.2, resolem aquest problema donant una caracterització de $J(v)$ en funció dels polinomis de 2-torsió, 3-torsió (segons si $v|3$ o $v|2$, respect.) d'una corba el·líptica amb invariant absolut j. Per a la demostració d'aquests teoremes, utilitzem algunes idees contingudes en el Capítol I.

Els casos $j = 0$, 1728, foren resolts per Neumann [Neum] així com la caracterització de $J(v)$ quan v és no-ramificat sobre 2 ó 3.

En la secció 2, tractem el problema global, és a dir, donat un $j \in K$ localment bo ($j \in J(v)$, per a tot v fora de S) trobem en el teorema 2.3 una condició necessària i suficient, senzilla i computable, per a que j sigui l'invariant j d'una corba el·líptica sobre K amb bona reducció arreu, fora de S. En la demostració d'aquest teorema ha estat fonamental el punt de vista de Neukirch [Neuk] sobre l'obstrucció global d'un problema local i l'aprofitament de la dualitat de Tate-Poitou. Els resultats d'aquest capítol foren anunciats a [Co2].

En la secció 1 del Capítol III, aquests resultats es fan molt més explícits per a corbes el·líptiques amb conductor trivial sobre cossos quadràtics (Teoremes 3.1, 3.2, 3.3). L'existència d'aquestes corbes fou primerament observada per Tate, després d'haver provat la seva no-existència sobre $\mathbb{Q}$ (cf. [Og1]).

Podem citar com a treballs pioners en aquest camp, els de Stroeker ([Stro]) i Setzer ([Set1], [Set2]) (vegi's també altres contribucions posteriors com: [Las], [Pi], [Krä], [Co1]).

En la secció 2, caracteritzem l'existència de corbes el·líptiques amb conductor trivial i model minimal global sobre K (cos quadràtic), en funció de la classe de Weierstraß de E, on E és una c.e. amb conductor trivial i $j(E) = j$. La demostració d'aquest resultat es basa simplement en les propietats de la classe de Steinitz d'una extensió quadràtica de K no-ramificada en els primers finits. Finalment, com a aplicació dels resultats del Capítol III, obtenim redemostracions de resultats ja obtinguts per Setzer [Set2] i Stroeker [Stro], així com d'altres resultats especials.

Com a conseqüència del corol·lari 3.2.1, provem que no existeixen corbes el·líptiques en un cos quadràtic amb conductor trivial i invariant j amb traça nul·la.

Suposant el nombre de classes de K primer amb 6, donem condicions necessàries i suficients per a la realització de les solucions enteres (x, y) de l'equació el·líptica:

$$y^2 = x^3 - 1728u, \qquad u \in \mathcal{U}_K, \qquad x,\, y \in \mathcal{O}_K$$

com a coeficients de Weierstraß c_4, c_6 (resp.) d'una corba el·líptica definida sobre $\mathcal{O}_K$.

Notem que aquest és un problema de realització global dels coeficients c_4, c_6, en contrast amb el problema de realització local, ja resolt per Kraus [Kra].

Cal dir que els resultats continguts en els Capítols II, III són efectius, en tant que donat un subconjunt finit de K ens permeten decidir i trobar tots els elements seus que són invariants j d'alguna corba el·líptica sobre K amb bona reducció fora de S.

Tots els resultats que apareixen etiquetats a la Memòria són originals, tret de les proposicions 2.1, 2.2, dels exemples 3 i 4, dels lemes 3.1, 3.3 i, potser, del lema 3.2.

En quant a notació, al llarg de la Memòria sempre K denotarà un cos de nombres. $\mathcal{O}_K, \mathcal{U}_K$ els seus anell d'enters i grup d'unitats respectius.

Σ serà el conjunt de les valoracions discretes de K.

Donada $v \in \Sigma$, normalitzada per $v(K^*) = \mathbf{Z}$, notarem per K_v, $\mathcal{O}_v$, $\mathcal{U}_v$, la compleció a v i l'anell dels enters i el grup d'unitats corresponent.

π serà un uniformitzant per $\mathcal{O}_v$ i $k_v = \mathcal{O}_v/(\pi)$ el cos residual. Finalment, posarem:

$$p = \mathrm{char}(k_v), \qquad e = v(p).$$

Vull agrair a en Gerhard Frey, Joseph H. Silverman i Glenn Stevens el seu interès i la seva amabilitat, així com a en Peter Schneider les seves indicacions tan oportunes sobre un article de Neukirch.

Dono les gràcies, també, a tot l'equip del Seminari de Teoria de Nombres de Barcelona, que any rera any m'ha anat contagiant del seu entusiasme per aquest món de les corbes el·líptiques.

Tots els consells que l'Enric Nart m'ha volgut donar han estat decisius per a la realització d'aquest treball i també per a la meva formació. A ell li estic especialment agraït.

CAPÍTOL 0. PRELIMINARS.

Aquestes pàgines pretenen ser només un breu recull d'algunes definicions i resultats bàsics en la teoria de les corbes el·líptiques i que han estat fonaments per al nostre treball.

Per a més detalls us remitim a la bibliografia ([Ta1], [Ta2], [Sil2], [Hu], [Né]).

1. *Equació de Weierstraß d'una corba el·líptica.*

Una corba el·líptica sobre K : $E|K$, és una parella (E,O) on E és una corba no-singular de gènere 1 definida sobre K i O és un punt K-racional de E (l'element neutre del grup dels punts de E). Tota corba el·líptica $E|K$ té un model pla cúbic de la forma:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

on $a_i \in K$ i x, y denoten les coordenades en el pla afí. Un tal model s'anomena equació de Weierstraß (afí) de $E|K$. Seguint la notació de Tate (cf. [Ta1]) definim els següents coeficients:

$$\begin{array}{ll} b_2 = a_1^2 + 4a_2 & b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\ b_4 = a_1a_3 + 2a_4 & c_4 = b_2^2 - 24b_4 \\ b_6 = a_3^2 + 4a_6 & c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \end{array}$$

Definim, també, les següents quantitats:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \qquad j = \frac{c_4^3}{\Delta}.$$

Δ s'anomena el discriminant de l'equació de Weierstraß i j, l'invariant j o invariant absolut de E.

Es tenen les relacions:

$$4b_8 = b_2b_6 - b_4^2, \qquad 1728\Delta = c_4^3 - c_6^2.$$

Finalment, posem:

$$w = \frac{dx}{2y + a_1x + a_3}$$

$$\gamma \equiv \begin{cases} \dfrac{-c_4}{c_6} \pmod{K^{*^2}} & \text{si } c_4c_6 \neq 0 \\ c_4 \pmod{K^{*^4}} & \text{si } c_6 = 0 (\Longleftrightarrow j = 1728) \\ c_6 \pmod{K^{*^6}} & \text{si } c_4 = 0 (\Longleftrightarrow j = 0) \end{cases}$$

w s'anomena l'invariant diferencial associat a l'equació de Weierstraß. γ s'anomena l'invariant γ o l'invariant de Hasse de $E|K$.

Un model de Weierstraß de $E|K$ és únic llevat d'una transformació de coordenades de la forma:

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t, \end{aligned}$$

amb r, s, t, $u \in K$, $u \neq 0$.

Fent aquest canvi, obtenim una nova equació de Weierstraß per a $E|K$:

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

i es satisfan les relacions següents:

$$\begin{aligned} ua_1' &= a_1 + 2s \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\ u^3a_3' &= a_3 + ra_1 + 2t \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \\ u^2b_2' &= b_2 + 12r \\ u^4b_4' &= b_4 + rb_2 + 6r^2 \\ u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \end{aligned}$$

$$\begin{aligned} u^4c_4' &= c_4, & u^{12}\Delta' &= \Delta, & u^{-1}w' &= w \\ u^6c_6' &= c_6, & j' &= j, & \gamma' &\equiv \gamma. \end{aligned}$$

Fent els canvis de coordenades:

$$\begin{aligned} &\text{(i)} && r = 0, && s = -a_1/2, && t = -a_3/2, && u = \frac{1}{2} \\ &\text{(ii)} && r = \frac{-b_2}{12}, && s = -a_1/2, && t = \frac{-a_3}{2} + \frac{a_1b_2}{24}, && u = \frac{1}{6} \end{aligned}$$

podem aconseguir unes equacions de Weierstraß *curtes* per a $E|K$, del tipus:

$$y^2 = x^3 + Ax^2 + Bx + C$$

on

$$\begin{aligned} &\text{(i)} && A = b_2, && B = 8b_4, && C = 16b_6 \\ &\text{(ii)} && A = 0, && B = -27c_4, && C = -54c_6. \end{aligned}$$

REMARQUES:

1) Sempre que utilitzem un canvi de coordenades amb $r = s = t = 0$, $u \in K^*$, direm que estem *dividint* l'equació de Weierstraß per u.
2) Hem vist, per les fórmules anteriors, que si E i E' són corbes el·líptiques isomorfes aleshores $j = j'$. Utilitzant les mateixes fórmules, no és difícil veure que el recíproc també és cert (sobre la clausura algebraica: $\bar{K}$). De fet, els invariants (j, γ) ens parametritzen les classes d'isomorfisme de corbes el·líptiques sobre K (veure torcements).

2. *El grup d'automorfismes.*

Sigui $E|K$ una corba el·líptica i posem:

$$n = \begin{cases} 2 & \text{si } j(E) \neq 0, 1728 \\ 4 & \text{si } j(E) = 1728 \\ 6 & \text{si } j(E) = 0 \end{cases}$$

μ_n, $G_{\bar{K}|K}$ denoten el grup de les arrels n-èssimes de la unitat i el grup de Galois absolut de K, respectivament. Aleshores es té el següent isomorfisme de $G_{\bar{K}|K}$-mòduls:

$$\mathrm{Aut}(E) \cong \mu_n.$$

Utilitzant equacions curtes de Weierstraß per a E, es prova fàcilment que l'aplicació:

$$\begin{aligned} [\,] : \mu_n &\longrightarrow \mathrm{Aut}(E) \\ \zeta &\longrightarrow [\zeta](x, y) = (\zeta^2 x, \zeta^3 y) \end{aligned}$$

és un isomorfisme de grups, que commuta clarament amb l'acció de $G_{\bar{K}|K}$.

3. *Equació de Weierstraß v-minimal. Discriminant minimal.*

Fixem $v \in \Sigma$ i considerem una equació de Weierstraß de $E|K_v$ amb coeficients $a_i \in \mathcal{O}_v$. Diem que aquesta equació és v-minimal si $v(\Delta)$ és mínima. Quan $p \neq 2, 3$ hi ha un criteri de v-minimalitat molt senzill:

L'equació de Weierstraß de $E|\mathcal{O}_v$ és v-minimal

$$\Longleftrightarrow v(\Delta) < 12 \text{ o } v(c_4) < 4.$$

En general, hi ha un algorisme de Tate (cf. [Ta2]) que determina si una certa equació és minimal.

El discriminant minimal de $E|K$ es defineix com l'ideal enter de K següent:

$$\mathcal{D}(E|K) = \left(\sum_{v \in \Sigma} v(\Delta_v) \cdot v \right)$$

on Δ_v és el discriminant d'una equació de Weierstraß v-minimal de E.

Un model minimal global per a $E|K$ és una equació de Weierstraß amb coeficients $a_i \in \mathcal{O}_K$ i discriminant Δ satisfent: $(\Delta) = \mathcal{D}(E|K)$.

Si K té nombre de classes 1, tota corba el·líptica sobre K té model minimal global. En general, l'existència d'aquest model vé caracteritzada per la classe de Weiestraß de $E|K$ (Vegi's Capítol III).

4. *Reducció.*

Fixat $v \in \Sigma$ i donada una equació de Weierstraß v-minimal de $E|K_v$, sigui $\tilde{E}$ la corba reduïda, és a dir, la corba obtinguda reduint els coeficients de l'equació mòdul π. Aleshores:

(a) Diem que E té bona reducció a v (o sobre K_v) si $\tilde{E}$ és no-singular (és a dir, és una corba el·líptica sobre k_v) $\iff v(\Delta) = 0$.

(b) Diem que E té reducció multiplicativa a v (o sobre K_v) si $\tilde{E}$ és singular i té un node $\iff v(\Delta) > 0$, $v(c_4) = 0$.

(c) Diem que E té reducció additiva a v (o sobre K_v) si $\tilde{E}$ és singular i té una punta $\iff v(\Delta) > 0$, $v(c_4) > 0$.

En els casos (b) i (c) diem que E té mala reducció a v.

Si $E|K$ té reducció bona o multiplicativa a tot $v \in \Sigma$ direm que E té reducció semistable (a K).

La variació en la reducció d'una corba el·líptica quan es fa una extensió del cos base ve donada pel següent:

TEOREMA (DE LA REDUCCIÓ SEMISTABLE).
Sigui $E|K_v$ una corba el·líptica.

(i) *Si $L|K_v$ és una extensió no-ramificada, aleshores E té la mateixa reducció (bona, multiplicativa o additiva) sobre K_v i sobre L.*

(ii) *Si $L|K_v$ és una extensió finita i E té reducció bona o multiplicativa sobre K_v, aleshores conserva la mateixa reducció sobre L.*

(iii) *Existeix una extensió finita $L|K_v$ tal que E té reducció bona o multiplicativa sobre L.*

Finalment, direm que E té bona reducció potencial a v (o sobre K_v) si existeix una extensió finita $L|K_v$ tal que E té bona reducció sobre L.

És senzill veure que E té bona reducció potencial a v si i sols si $j(E) \in \mathcal{O}_v$.

5. *El model v-regular, v-minimal.*

Quan es considera la corba el·líptica $E|K_v$ com un esquema $E \longrightarrow \mathrm{Spec}(\mathcal{O}_v)$, definit per l'equació de Weierstraß v-minimal, pot resultar ser un esquema no-regular (per exemple, si E té mala reducció a v). Resolvent les possibles sin-

gularitats de E, es demostra (cf. [Né]) que es pot obtenir un esquema projectiu de dimensió 2 $\mathcal{C}/\mathrm{Spec}(\mathcal{O}_v)$, regular, la fibra genèrica, $\mathcal{C} \underset{\mathrm{Spec}(\mathcal{O}_v)}{\times} \mathrm{Spec}(K_v)$, del qual és isomorfa a E/K_v (sobre K_v), i minimal respecte a l'aplicació $\mathcal{C} \longrightarrow \mathrm{Spec}(\mathcal{O}_v)$ (és a dir, no pot existir una factorització $\mathcal{C} \longrightarrow \mathcal{C}' \longrightarrow \mathrm{Spec}(\mathcal{O}_v)$ tal que $\mathcal{C} \underset{\mathrm{Spec}(\mathcal{O}_v)}{\times} \mathrm{Spec}(K_v) \xrightarrow{\sim} \mathcal{C}' \underset{\mathrm{Spec}(\mathcal{O}_v)}{\times} \mathrm{Spec}(K_v)$ sigui isomorfisme). Un esquema $\mathcal{C}$ amb aquestes propietats és únic, llevat d'isomorfismes. $\mathcal{C}$ s'anomena el model v-regular v-minimal de E sobre K_v (també, per alguns autors, el model minimal de Néron de E sobre K_v). La seva fibra especial $\tilde{\mathcal{C}} = \mathcal{C} \underset{\mathrm{Spec}(\mathcal{O}_v)}{\times} \mathrm{Spec}(k_v)$ presenta un dels 10 tipus que apareixen a la taula 1. Per a conèixer el tipus de la fibra especial -que notarem d'ara endavant $\mathrm{tip}_v(E)$ o, simplement, $\mathrm{tip}(E)$ si $v \in \Sigma$ és fixada- cal disposar d'una equació de Weierstraß v-minimal de la corba E.

Si $p \neq 2, 3$, això ens permet llegir directament el seu tipus a la taula 1.

Si, per contra, $p = 2, 3$, haurem de reduir l'equació inicial a un dels 10 models minimals que apareixen a la taula i que s'anomenen models v-estàndard.

En general, hom pot trobar (per a qualsevol p), un model v-estàndard (i, per tant, una equació minimal) de E mitjançant l'algorisme de Tate ([Ta2]) a partir d'una equació de Weierstraß sobre $\mathcal{O}_v$ qualsevol.

REMARQUES (TAULA 1):

1. En aquesta Memòria utilitzarem només els símbols de Kodaira i posarem:

$$\mathrm{tip}_v(E) = (\text{símbol de Kodaira corresp.})$$

per a expressar el tipus de $\tilde{\mathcal{C}}$ (a $v \in \Sigma$).

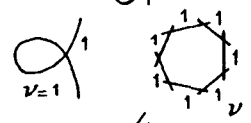
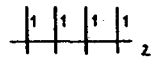
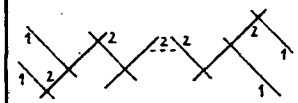
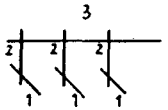
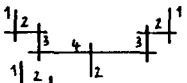
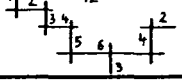
2. Per a $p = 2$, $v \in \Sigma$ i $\mathrm{tip}_v(E) = \mathrm{I}_0^*$, es té, per un model v-estàndard de E:

$$v(\tilde{\Delta}) = 6 \Longleftrightarrow v(a_6 - a_2 a_4) = 3.$$

En efecte, el resultat és immediat a partir de la igualtat:

$$\tilde{\Delta} = a_2^2 a_4^2 - 4a_4^3 - 4a_2^3 a_6 - 27a_6^2 + 18a_2 a_4 a_6.$$

Taula 1

$tip_v(E)$	model v-estàndard	$p \neq 2$	$\widetilde{C}/\overline{k}_v$	m_v	c
I_0 (A)	$v(\Delta) = 0$	$v(\Delta) = 0$		1	1
I_ν (B_ν)	$v(b_2) = 0 \quad v(a_3) > \frac{\nu}{2} \quad v(a_4) > \frac{\nu}{2} \quad v(a_6) = \nu$	$v(\Delta) = \nu \quad v(j) = -\nu$		ν	ν
II $(C1)$	$v(a_6) = 1$	$p \neq 3 : v(\Delta) = 2 \quad v(j) \geq 0$		1	1
III $(C2)$	$v(a_4) = 1 \quad v(a_6) \geq 2$	$v(\Delta) = 3 \quad v(j) \geq 0$		2	2
IV $(C3)$	$v(a_4) \geq 2 \quad v(a_6) \geq 2 \quad v(b_6) = 2$	$p \neq 3 : v(\Delta) = 4 \quad v(j) \geq 0$		3	3
I_0^* $(C4)$	$v(a_3) \geq 2 \quad v(a_4) \geq 2 \quad v(a_6) \geq 3 \quad v(\widetilde{\Delta}) = 6$	$v(\Delta) = 6 \quad v(j) \geq 0$		5	2×2
I_ν^* $(C5_\nu)$		$v(\Delta) = \nu + 6 \quad v(j) = -\nu$		$\nu + 5$	
$\nu = 2n - 1$	$v(a_3) \geq n + 1 \quad v(a_2) = 1 \quad v(a_4) \geq n + 2 \quad v(a_6) \geq 2n + 2 \quad v(b_6) = 2n + 2$				4
$\nu = 2n$	$v(a_3) \geq n + 2 \quad v(a_2) = 1 \quad v(a_4) \geq n + 2 \quad v(a_6) \geq 2n + 3 \quad v(\widetilde{\delta}) = 2n + 4$		$\nu + 1$ comp. dobles		2×2
IV^* $(C6)$	$v(a_3) \geq 2 \quad v(a_2) \geq 2 \quad v(a_4) \geq 3 \quad v(a_6) \geq 4 \quad v(b_6) = 4$	$p \neq 3 : v(\Delta) = 8 \quad v(j) \geq 0$		7	3
III^* $(C7)$	$v(a_3) \geq 3 \quad v(a_2) \geq 2 \quad v(a_4) = 3 \quad v(a_6) \geq 5$	$v(\Delta) = 9 \quad v(j) \geq 0$		8	2
II^* $(C8)$	$v(a_3) \geq 3 \quad v(a_2) \geq 2 \quad v(a_4) \geq 4 \quad v(a_6) = 5$	$p \neq 3 : v(\Delta) = 10 \quad v(j) \geq 0$		9	1

$tip_v(E)$: símbol de Kodaira(Néron) . $v(a_i) \geq 0$. Si $tip_v(E) \neq I_0, I_\nu : v(a_i) \geq 1$. $\widetilde{\Delta} := disc(T^3 + a_2T^2 + a_4T + a_6)$; $\widetilde{\delta} := a_4^2 - 4a_2a_6$.
$m_v :=$ nombre de comp. irreductibles de la fibra especial (sense multiplicitats) . $c := [E(K_v) : E_0(K_v)]$

6. *Torcements.*

Sigui $E|K$ una corba el·líptica. Un torcement de E és una corba el·líptica $E|K$ tal que E i E' són isomorfes a $\bar{K}$.

Considerem el conjunt $\mathrm{Twist}(E)$ de corbes el·líptiques que són torcements de E, identificant-les mòdul K-isomorfisme. Tenim, de fet, que:

$$\mathrm{Twist}(E) = \{E'|K(\mathrm{mod}\ K\text{-isom.});\ j(E') = j(E)\}.$$

Donada $E' \in \mathrm{Twist}(E)$, sigui $\Phi : E' \longrightarrow E$ un $\bar{K}$-isomorfisme de corbes el·líptiques. Aleshores, hom pot considerar el 1-cocicle:

$$\begin{aligned} \zeta : G_{\bar{K}|K} &\longrightarrow \mathrm{Aut}(E) \\ \sigma &\longrightarrow \Phi^{\sigma} \circ \Phi^{-1} \end{aligned}$$

i la seva classe $[\zeta] \in H^1(G_{\bar{K}|K}, \mathrm{Aut}(E))$.

Recíprocament, donat un 1-cocicle ζ, hom pot considerar el cos de funcions de $E : \bar{K}(E)_{\zeta}$ amb l'acció de $G_{\bar{K}|K}$ *torçada per* ζ, és a dir:

$$\sigma \in G_{\bar{K}|K},\ f \in \bar{K}(E)_{\zeta} : \quad f^{\sigma} := \sigma(f)\zeta(\sigma).$$

Sigui $F = \bar{K}(E)_{\zeta}^{G_{\bar{K}|K}}$, el subcos fix per aquesta acció. Aleshores es demostra que:

(i) Existeix $E' \in \mathrm{Twist}(E)$; $F \cong K(E')$.

(ii) Les assignacions anteriors donen una bijecció:

$$\mathrm{Twist}(E) \Longleftrightarrow H^1(G_{\bar{K}|K}, \mathrm{Aut}(E)).$$

Sigui n com en l'apartat 2. De l'isomorfisme $\mathrm{Aut}(E) \cong \mu_n$ tenim:

$$H^1(G_{\bar{K}|K}, \mathrm{Aut}(E)) \cong H^1(G_{\bar{K}|K}, \mu_n) \cong K^*/K^{*^n}$$

i d'aquí concloem que $\mathrm{Twist}(E)$ és canònicament isomorf a K^*/K^{*^n}. L'isomorfisme ve donat per:

$$\begin{aligned} \Gamma : \mathrm{Twist}(E) &\longrightarrow K^*/K^{*^n} \\ E' &\longrightarrow \gamma(E')/\gamma(E) \end{aligned}$$

essent γ, l'invariant γ definit a l'apartat 1.

Donat $D \in K^*/K^{*^n}$, podem definir, doncs, la corba *torçada* de E per D com:

$$E^D := \Gamma^{-1}(D).$$

Concretament, si escollim una equació de Weierstraß per a E curta, del tipus

$$y^2 = x^3 + ax + b,$$

aleshores la corba E^D presenta la següent equació de Weierstraß:

$$\begin{array}{ll} y^2 = x^3 + D^2ax + D^3b, & \text{si } j(E) \neq 0, 1728 \\ y^2 = x^3 + Dax, & \text{si } j(E) = 1728 \\ y^2 = x^3 + Db, & \text{si } j(E) = 0. \end{array}$$

Suposem $\mu_n \subset K$ i sigui

$$\chi : G_{\bar{K}|K} \longrightarrow \mu_n$$

un caràcter corresponent a una extensió $K(\sqrt[n]{D})|K$, $D \in K^*/K^{*^n}$. Podem definir, de manera equivalent, el torcement de E pel caràcter χ com:

$$E^\chi := E^D.$$

Si considerem χ com a cocicle i la seva classe dins $H^1(G_{\bar{K}|K}, \mathrm{Aut}(E))$:

$$\begin{array}{rl} \chi : G_{\bar{K}|K} \longrightarrow \mu_n & \xrightarrow{\sim} \mathrm{Aut}(E) \\ \sigma \longrightarrow \chi(\sigma) & \longrightarrow [\chi(\sigma)](x,y) = (\chi^2(\sigma)x,\, \chi^3(\sigma)y), \end{array}$$

aleshores, existeix un $\bar{K}$-isomorfisme

$$\Phi : E^\chi \longrightarrow E \text{ tal que}$$

$$\Phi^\sigma \circ \Phi^{-1}(x,y) = (\chi^2(\sigma)x, \chi^3(\sigma)y)$$

per a tot $\sigma \in G_{\bar{K}|K}$, $P \in E$, $P = (x,y)$.

Quan $n = 2$ (χ caràcter quadràtic), l'acció de $G_{\bar{K}|K}$ sobre Φ vindrà donada per:

$$\Phi^\sigma \circ \Phi^{-1}(P) = \chi(\sigma) \cdot P$$

o, equivalentment,

$$(\Phi(P))^\sigma = \chi(\sigma) \cdot \Phi(P^\sigma)$$

per a tot $\sigma \in G_{\bar{K}|K}$, $P \in E$.

CAPÍTOL I. TIPUS DE REDUCCIÓ DELS TORCEMENTS.

Sigui K un cos de nombres i $E|K$ una corba el·líptica definida sobre K. Considerem una extensió quadràtica amb caràcter χ i notem E^χ el torcement de E per χ. El nostre objectiu és:

(1) Estudiar la relació entre el tipus de reducció de la corba E i el de la corba E^χ.
(2) Donar una fórmula que expliciti la relació entre els discriminants minimals d'ambdues corbes.

§1. Els casos no-ramificat i semistable.

Sigui $D \in K^*/K^{*n}$, $n = 2, 4, 6$, i considerem el torcement de E per D, que notem E^D. Fixem $v \in \Sigma$ i posem $L = K(\sqrt[n]{D})$.

PROPOSICIÓ.

(i) *Si $L|K$ és no-ramificada a v, E i E^D tenen el mateix tipus de reducció a v.*
(ii) *Si $L|K$ és ramificada a v i E hi té reducció semistable, aleshores E^D hi té mala reducció additiva.*

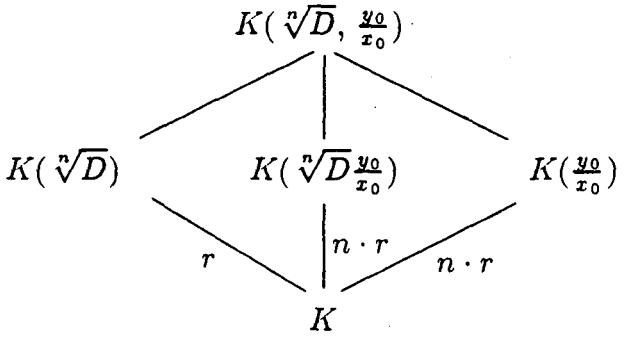
DEMOSTRACIÓ:

L'apartat (i) és conseqüència immediata del teorema de la reducció semistable i del fet que E i E^D són isomorfes a L.

Per a provar (ii), suposem que E^D tingués bona reducció a v. Llavors considerem un punt $P \in E[l]$, on $(l,p) = 1$. Sigui $\Phi : E^D \longrightarrow E$ el $\bar{K}$-isomorfisme tal que:

$$\Phi^{-1}(x,y) = ((\sqrt[n]{D})^2 x, (\sqrt[n]{D})^3 y).$$

Posem, doncs, $P = (x_0, y_0)$ i escollim-lo tal que $x_0 y_0 \neq 0$. Pel criteri de Néron-Ogg-Šafarevič (cf. [Ta1], [Sil2], per exemple) tindrem que les extensions $K(x_0, y_0)|K$ i $K((\sqrt[n]{D})^2 x_0, (\sqrt[n]{D})^3 y_0)|K$ són ambdues no-ramificades a v, fet que és contradictori:



Finalment, suposem que E té reducció multiplicativa a v, i considerem, per l prou gran, $\tilde{\rho}_l$, $\tilde{\rho}_{l,\chi}$, les representacions mòdul l associades a E, E^χ, respectivament, on χ és el caràcter quadràtic de l'extensió $L|K$. Siguin G_i, H_i, $i \geq 0$, els grups de ramificació corresponents a $G_{\bar{K}_v|K_v}$, $G_{\bar{K}_v|L_w}$, respectivament. Aleshores:

$$\dim_{\mathbb{F}_l} E[l]/E[l]^{G_0} = 1.$$

Quan $p = 2$, el nombre de grups de ramificació de l'extensió $L_w|K_v$ és 2e ó $2(e-k)-1(k<e)$, en particular, és més gran o igual que 1. Per tant, el grup:

$$\left(\frac{G_{\bar{K}_v|K_v}}{G_{\bar{K}_v|L_w}}\right)_1 \cong \frac{G_1}{H_1}$$

és no-trivial. Així, $\chi(G_1) = \{\pm 1\}$. Per tenir E reducció multiplicativa a v, $\tilde{\rho}_l$ és moderadament ramificada a v, és a dir, $\tilde{\rho}_l(G_1)$ és trivial. Per tant, $\tilde{\rho}_{l,\chi}(G_1) = \chi(G_1)\cdot\tilde{\rho}_l(G_1)$ és no-trivial. Aleshores, E^χ no pot tenir reducció multiplicativa.

Suposem, doncs, $p \neq 2$. En aquest cas, el nombre de grups de ramificació de $L_w|K_v$ és 1 i, per tant, $\dfrac{G_1}{H_1}$ és trivial. Com que $\dim_{\mathbb{F}_l} E[l]^{G_0} = 1$, podem escollir una base de la l-torsió tal que la representació s'escrigui:

$$\tilde{\rho}_l(\sigma) = \begin{pmatrix} 1 & \alpha(\sigma) \\ 0 & \beta(\sigma) \end{pmatrix}, \qquad \beta(\sigma) \neq 0, \qquad \sigma \in G_0.$$

Sigui σ_0 un generador del grup cíclic $\dfrac{G_0}{G_1}$. Llavors, hem de tenir $\beta(\sigma_0) = -1$. En efecte, ja que si $\beta(\sigma_0) = -1$, de $G_0/H_0 \cong \mathbb{Z}/2\mathbb{Z}$ i el fet que $\tilde{\rho}_l(\sigma_0^{2r}) = \mathrm{id}\ \forall r \in \mathbb{Z}$, obtenim que $\tilde{\rho}_l(H_0) = \mathrm{id}$. Però en aquest cas,

$$\tilde{\rho}_{l,\chi}(H_0) = \chi(H_0)\tilde{\rho}_l(H_0) = \mathrm{id}$$

i això contradiu el fet que E^χ té reducció multiplicativa a L_w (i no bona reducció).

Concloem, doncs, que $\tilde{\rho}_{l,\chi}(\sigma_0) = \begin{pmatrix} -1 & -\alpha(\sigma_0) \\ 0 & -\beta(\sigma_0) \end{pmatrix}$ amb $-\beta(\sigma_0) \neq 1$. Però aquesta matriu no deixa fix a ningú (llevat del (0,0)). Per tant, $\dim_{\mathbb{F}_l} E^\chi[l]^{G_0} = 0$. És a dir, E^χ té reducció additiva a v (cf. [Ba-La], [STN]) ∎

COROL·LARI.

Suposem que E tingui reducció semistable a v. Aleshores E i E^D tenen el mateix tipus de reducció si i sols si $L|K$ és no-ramificada a v.

§2. La fórmula dels discriminants minimals.

Sigui $L|K$ una extensió quadràtica amb caràcter χ. Suposem que $L|K$ és no-ramificada a tots els primers de K que divideixen 2 i a tots els primers en els quals E té mala reducció. En aquestes hipòtesis, Silverman prova [Sil1, Th.3] la següent relació entre els discriminants minimals de E i E^χ:

$$\mathcal{D}(E^\chi|K) = \mathcal{D}^6(\chi) \cdot \mathcal{D}(E|K) \tag{1.1}$$

on $\mathcal{D}(\chi)$ és el discriminant de l'extensió $L|K$.

De fet, la fórmula anterior continua essent certa en el cas que χ sigui ramificat en algun primer en el qual E hi tingui reducció multiplicativa. Això es pot veure resseguint la mateixa demostració que dóna Silverman.

Quan hom intenta llevar més condicions sobre la ramificació de χ aparèixen ja anomalies. Així ho veié Stevens [Ste] quan va calcular, per $K = \mathbb{Q}$, una fórmula suposant només χ no-ramificat sobre els primers de reducció additiva de E, obtenint:

$$\mathcal{D}(E^\chi|\mathbb{Q}) = \eta^{-12} \cdot \mathcal{D}^6(\chi) \cdot \mathcal{D}(E|\mathbb{Q})$$

on

$$\eta = \begin{cases} 2 & \text{si } 8|\mathcal{D}(\chi) \text{ i } E \text{ té b.r. supersingular al 2} \\ 1 & \text{en altre cas.} \end{cases}$$

Anem a tractar alhora les dues qüestions plantejades a l'inici del capítol, mitjançant l'algoritme de Tate. Fixat $v \in \Sigma$ i donada una corba el·líptica E, amb un determinat model v-estàndard, i un caràcter quadràtic χ qualsevol, trobarem el model v-estàndard de la corba E^χ i la relació entre els dos discriminants minimals que denotarem localment per h_v, on:

$$12h_v = v(\mathcal{D}(E|K)) + 6v(\mathcal{D}(\chi)) - v(\mathcal{D}(E^\chi|K)).$$

h_v serà, doncs, el factor de correcció local de la fórmula (1.1). Per tant, la fórmula global entre els discriminants minimals es podrà escriure:

$$\mathcal{D}(E^\chi|K) = \eta^{-12} \cdot \mathcal{D}^6(\chi) \cdot \mathcal{D}(E|K)$$

amb $v(\eta) = h_v$, per a tot $v \in \Sigma$.

REMARQUES:

1. Notem que sempre es té:

$$v(\mathcal{D}(E|K)) + 6v(\mathcal{D}(\chi)) - v(\mathcal{D}(E^\chi|K)) \equiv 0 \pmod{12}.$$

En efecte, si Δ_v, Δ_v^χ són els discriminants de dos models v-minimals de E, E^χ, respectivament, aleshores:

$$v(\Delta_v^\chi) \equiv v(d^6\Delta_v) \pmod{12}$$

mentre que $v(\mathcal{D}(\chi)) \equiv v(d) \pmod 2$, per a tot $v \in \Sigma$.

2. En la demostració del teorema de la reducció semistable, es prova, de fet, que si χ és no-ramificat a v, aleshores E^χ presenta el mateix tipus v-estàndard que E, és a dir, $\text{tip}(E^\chi) = \text{tip}(E)$ a v. A més, la fórmula de Silverman (1.1) ens diu que $h_v = 0$. Per tant, suposarem a partir d'ara χ ramificat a v.

PROPOSICIÓ.

Suposem $p \neq 2$ i sigui $v \in \Sigma$ i χ un caràcter quadràtic ramificat a v. Aleshores es té el resultat següent:

$\text{tip}(E)$	$\text{tip}(E^\chi)$	h_v
I_0	I_0^*	0
I_ν	I_ν^*	0
II	IV*	0
III	III*	0
IV	II*	0
I_0^*	I_0	1
I_ν^*	I_ν	1
IV*	II	1
III*	III	1
II*	IV	1

DEMOSTRACIÓ:

Per ésser $p \neq 2$, podem aconseguir sempre un model de Weierstraß v-estàndard, de la forma:

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Per tant, la corba E^χ tindrà un model:

$$y^2 = x^3 + a_2dx^2 + a_4d^2x + a_6d^3, \qquad d \in K^*/K^{*^2}, \qquad v(d) = 1. \tag{1.2}$$

Si E presenta un dels cinc primers tipus v-estàndard, el model (1.2) resulta ser minimal i el seu tipus es llegeix de manera directa a la taula 1.

En els altres casos obtenim el model minimal, dividint (1.2) per $u = \pi$. Finalment, per a calcular el nombre de components de la fibra especial en els models I_ν, I_ν^*, utilitzem la igualtat $v(j) = -\nu$, que també es satisfà en característica 3 ∎

Suposarem, d'ara endavant, $p = 2$. Fixem $v \in \Sigma$. Donat $\alpha \in K^*/K^{*^2}$, notarem:

$$\delta(\alpha) := v(\mathcal{D}(K(\sqrt{\alpha})|K)).$$

Sigui E una corba el·líptica sobre K i considerem una extensió quadràtica $K(\sqrt{d})|K$ ramificada a v, amb caràcter χ. Podem suposar, sense restricció, $v(d) = 0, 1$.

REMARQUES 1:

1. Es té, per tant, $\delta(d) = \begin{cases} 2e+1 & \text{si } v(d)=1 \\ 2(e-k),\ k \leq e, & \text{si } v(d)=0 \end{cases}$
2. Suposem $v(d) = 0$, $\delta(d) = 2(e-k)$, $k < e$.
   Aleshores existeix $x \in \mathcal{O}_v$ tal que:
$$v(x^2 - d) = 2k + 1.$$
   En efecte, siguin $\mathcal{O}_w$, $\mathcal{O}_v$ els anells d'enters de $K_v(\sqrt{d})$, K_v, respectivament. Llavors, existeixen a, $b \in \mathcal{O}_v$, $(a, b, \pi) = 1$ tals que:
$$\mathcal{O}_w = \mathcal{O}_v \left[1, \frac{a + b\sqrt{d}}{\pi^k}\right]$$
   i $w\left(\dfrac{a+b\sqrt{d}}{\pi^k}\right) = 1$ (cf. [Nar], [Se]). Prenent normes, obtenim:
$$v(a^2 - b^2 d) = 2k + 1.$$
3. Recíprocament, essent $v(d) = 0$, suposem que existeix $x \in \mathcal{O}_v$ amb $v(x^2 - d) = 2i + 1$, $0 \leq i < e$. Aleshores, $\delta(d) = 2(e-i)$.
   En efecte, suposem que existís $y \in \mathcal{O}_v$ tal que:
$$y^2 = d \pmod{\pi^{2k}} \text{ amb } i < k \leq e.$$
   Llavors, $v(x^2 - y^2) = 2i + 1$ però d'aquí: $v(x-y) + v(x-y+2y) \geq 2i + 2$!

Definim les constants α_E, β_E associades a E com:

$$\alpha_E = \begin{cases} 1 & \text{si tip}(E) = \text{IV}^*, \text{III}^*, \text{II}^* \\ 0 & \text{en altre cas} \end{cases}$$

$$\beta_E = \begin{cases} 4 & \text{si tip}(E) = \text{II}^* \\ 3 & \text{si tip}(E) = \text{III}^* \\ 2 & \text{si tip}(E) = \text{IV}^*, \text{I}_\nu^*, \text{I}_0^* \\ 0 & \text{en altre cas.} \end{cases}$$

LEMA 1.1. *Suposem $p = 2$, $v \in \Sigma$. Donada $c \in \mathbb{N}$, $c > 0$ i E una corba el·líptica sobre K, existeix un model de Weierstraß v-minimal de E, satisfent alguna de les següents condicions:*

(i) $v(b_8) \geq c$.
(ii) $v(b_8) < c$ *i* $v(b_8) \not\equiv 0$ *(mod 4) sempre que* $4v(b_6) > 3v(b_8)$ *i* $4v(b_2) > v(b_8)$.

DEMOSTRACIÓ:

Suposem $v(b_8) \leq c$, $v(b_8) \equiv 0 \pmod 4$ i $4v(b_6) > 3v(b_8)$, $4v(b_2) > v(b_8)$. De la relació:

$$4b_8 = b_2b_6 - b_4^2$$

tenim també: $2v(b_4) > v(b_8)$.

Sigui $\alpha \in K$ tal que $b_8 \equiv \alpha^4 \pmod{\pi^{v(b_8)+1}}$. Aleshores, fent el canvi de coordenades $r = \alpha$, obtenim un nou model de Weierstraß minimal per a E amb

$$v(b_8') > v(b_8) \blacksquare$$

En els enunciats i demostracions dels teoremes que segueixen, utilitzarem el següent model v-minimal per a E:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.3}$$

on els coeficients a_i vénen descrits pels models v-estàndard (veure taula 1) quan $\text{tip}(E) \neq \text{II}, \text{I}_0^*, \text{II}^*, \text{I}_\nu^*$, i en cas contrari vénen descrits pel següent lema:

LEMA 1.2. *Suposem $p = 2$, $v \in \Sigma$. Sigui E una corba el·líptica sobre K.*

(a) *Si $tip(E) = II, I_0^*, II^*$, existeix un model v-estàndard de E satisfent:*
  (a1) $v(b_8) \not\equiv 0$ *(mod 4) quan:* $v(b_2) \geq \delta(d) + \alpha_E$, $v(b_6) = \delta(d) + \beta_E$ *i* $3v(b_8) < 4v(b_6)$.
  (a2) $v(a_4) \geq 3$, $v(a_6) = 3$ *quan* $tip(E) = I_0^*$.

(b) *Si $tip(E) = I_\nu^*$, existeix un model v-minimal de E satisfent:*
  (b1) $v(a_3) \geq 2$, $v(a_2) = 1$, $v(a_4) \geq 3$, $v(a_6) \geq 4$.
  (b2) $v(b_8) \not\equiv 0$ *(mod 4) quan:* $v(b_2) = \delta(d)$, $v(b_6) \geq \delta(d) + 3$, $v(b_8) < 4\delta(d)$ *i* $3v(b_8) < 4v(b_6)$.
  (b3) $v(b_6) \neq 3\delta(d)$ *quan:* $v(b_2) = \delta(d)$ *i* $v(b_8) \geq 4\delta(d)$.

DEMOSTRACIÓ:

(a2) és conseqüència de l'equivalència:

$$v(\tilde{\Delta}) = 6 \Longleftrightarrow v(a_6 - a_2a_4) = 3$$

(veure remarques (taula 1)).

Per a provar (b3), suposem $v(b_6) = 3\delta(d)$. Sigui $r \in K$ t.q. $v(b_6 + r^2b_2) > 3\delta(d)$. Fem la traslació per aquest r per a obtenir el model desitjat.

Finalment, (a1) i (b2) són conseqüència immediata del lema 1.1 $\blacksquare$

Donada, doncs, la corba E amb model v-minimal (1.3), la corba E^χ té el model, no necessàriament minimal, següent:

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6' \tag{1.4}$$

on

$$a'_2 = db_2 \qquad a'_6 = 16d^3b_6$$
$$a'_4 = 8d^2b_4 \qquad \Delta' = 2^{12}d^6\Delta.$$

Si $v(d) = 0$, sigui $\alpha \in \mathcal{O}_v$ t.q.:

$$d \equiv \alpha^2 (\text{mod } \pi^{2e-\delta(d)+1}).$$

Aleshores, fent el canvi $s = a_1\alpha$, $t = 4da_3\alpha$, obtenim el següent model per a E^χ:

$$y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6 \tag{1.5}$$

on

$$\begin{aligned}
a'_1 &= 2a_1\alpha \\
a'_2 &= a_1^2(d - \alpha^2) + 4a_2d \\
a'_3 &= 8da_3\alpha \\
a'_4 &= 8d[a_1a_3(d - \alpha^2) + 2da_4] \\
a'_6 &= 16d^2[a_3^2(d - \alpha^2) + 4da_6] \\
\Delta' &= 2^{12}d^6\Delta.
\end{aligned}$$

TEOREMA 1.1. *Suposem $p = 2$. Sigui $v \in \Sigma$ i χ un caràcter quadràtic, associat a $d \in K^*/K^{*^2}$, ramificat a v. Sigui E una corba el·líptica sobre K, amb model v-minimal (1.3). Llavors, es té:*

(i) *Si $v(b_6) - \beta_E \leq \delta(d) \leq v(b_2) - \alpha_E$, $\delta(d) \neq v(b_6) - \beta_E$ quan $tip(E) = II$, I_0^*, II^*; o si $2(v(b_2) - \alpha_E) < 2\delta(d) < 3v(b_2) - v(b_6) + 3$, posem:*

$$v(b_6) + 2\delta(d) = i + 6l, \qquad 0 \leq i < 6. \text{ Aleshores:}$$

$tip(E^\chi) = II$, I_0^*, II^* segons $i = 0$, 2, 4 respectivament i $h_v = l$.

(ii) *Si $2\delta(d) \geq \max(3v(b_2) - v(b_6) + 3, 2(v(b_2) - \alpha_E + 1))$, aleshores:*

$$tip(E^\chi) = I_\nu^*, \qquad h_v = \frac{1}{2}v(b_2).$$

(iii) *Si $v(d) = 0$, $\delta(d) \leq \min(v(b_2) - \alpha_E, v(b_6) - \beta_E - 1))$, $\delta(d) \neq v(b_2)$ quan $tip(E) = I_\nu^*$, aleshores:*

$$tip(E^\chi) = tip(E), \qquad h_v = \frac{1}{2}\delta(d).$$

(iv) *Si $tip(E) = III$, III^*, $v(d) = 1$, $\delta(d) \leq \min(v(b_2) - \alpha_E, v(b_6) - \beta_E - 1)$. Aleshores es té:*

tip(E)	tip(E^χ)	h_v
III	III*	e
III*	III	e+1

DEMOSTRACIÓ:

De les hipòtesis de (i) obtenim les desigualtats següents:

$$3v(b_2) - v(b_6) \geq 2\delta(d) - 2$$

$$v(b_6) \leq \max(\delta(d) + 3\alpha_E - 1,\ \delta(d) + \beta_E).$$

Si $v(d) = 0$, torçant per χ obtenim un model (1.5) satisfent:

$$v(a_6') = 4e + v(b_6) + 2k + 1, \text{ on } \delta(d) = 2(e - k).$$

Posem $v(b_6) + 4e + 2k = i + 6(l + k)$, $i = 0, 2, 4$. Dividint per $u = \pi^{l+k}$ tenim:

$$v(a_6'u^{-6}) = i + 1 \qquad v(a_2'u^{-2}) \geq \frac{1+i}{3}$$
$$v(a_4'u^{-4}) \geq \frac{2i+3}{3} \qquad v(a_1'u^{-1}) \geq \frac{4+i}{3}$$
$$v(a_3'u^{-3}) \geq \frac{2+i}{3} \qquad v(\Delta'u^{-12}) = 12(e - k - l) + v(\Delta).$$

Si $v(d) = 1$, torçant per χ obtenim un model (1.4) satisfent:

$$v(a_6') = 4e + v(b_6) + 3.$$

Dividint per $u = \pi^l$ tenim:

$$v(a_6'u^{-6}) = i + 1$$
$$v(a_4'u^{-4}) = \frac{1}{3}\left(2i + 2 + e + 3v(b_4) - 2v(b_6)\right).$$

Si $v(b_4) \geq \dfrac{v(b_2b_6)}{2}$ aleshores $v(a_4'u^{-4}) \geq \dfrac{2i+4+3e}{3}$.

Si $v(b_4) < \dfrac{v(b_2b_6)}{2}$ aleshores de $4b_8 = b_2b_6 - b_4^2$ tenim $v(b_4) = e + \dfrac{v(b_8)}{2}$ i, en qualsevol cas, s'obté:

$$v(a_4'u^{-4}) \geq \frac{2i+3}{3}.$$

Finalment, $v(a_2'u^{-2}) \geq \dfrac{i+1}{3}$ i

$$v(\Delta'u^{-12}) = 12e + 6 + v(\Delta) - 12l.$$

Això prova (i).

De les hipòtesis de (ii) tenim:

$$v(b_2) = 2v(a_1),$$
$$v(a_3) \geq 3v(a_1) - \delta(d) + 2.$$

Si $v(d) = 0$, torçant per χ obtenim un model (1.5) satisfent:

$$v(a_2') = v(b_2) + 2k + 1, \text{ on } \delta(d) = 2(e-k).$$

Dividint per $u = \pi^{v(a_1)+k}$, obtenim:

$$v(a_1'u^{-1}) = e - k \qquad v(a_4'u^{-4}) \geq 3$$
$$v(a_2'u^{-2}) = 1 \qquad v(a_6'u^{-6}) \geq 4$$
$$v(a_3'u^{-3}) \geq 3 \qquad v(\Delta' u^{-12}) = 12e + v(\Delta) - 12(v(a_1) - k)$$
$$= 6\delta(d) + v(\Delta) - 6v(b_2).$$

Si $v(d) = 1$, obtenim un model (1.4) satisfent:

$$v(a_2') = v(b_2) + 1.$$

Dividint per $u = \pi^{v(a_1)}$ tenim:

$$v(a_2'u^{-2}) = 1$$
$$v(a_4'u^{-4}) = 3e + 2 + v(b_4) - 2v(b_2).$$

Si $\text{tip}(E) = \text{I}_0$ i $v(b_2) > 0$, aleshores $v(b_6) = 0$ i de les hipòtesis tenim:

$$3v(b_2) \leq 2\delta(d) - 4.$$

Si $\text{tip}(E) \neq \text{I}_0$ aleshores es té $v(b_4) \geq v(a_1) + 1$. En qualsevol cas, $v(a_4'u^{-4}) \geq 3$. Finalment,

$$v(a_6'u^{-6}) = 4e + 3 + v(b_6) - 3v(b_2) \geq 5$$
$$\text{i } v(\Delta' u^{-12}) = 12e + 6 + v(\Delta) - 6v(b_2).$$

Això prova (ii).

En les hipòtesis de (iii) tenim necessàriament: $\text{tip}(E) \neq \text{I}_0, \text{I}_\nu, \text{IV}, \text{IV}^*$. Obtenim, en torçar per χ, un model (1.5) amb:

$$v(a_1') = e + v(a_1)$$
$$v(a_2') = \begin{cases} 2e+1 & \text{si } \text{tip}(E) = \text{I}_v^* \\ \geq 2e + \alpha_E + 1 & \text{en altre cas} \end{cases}$$
$$v(a_3') = e + v(a_3)$$
$$v(a_4') = \begin{cases} 4e + v(a_4) & \text{si } \text{tip}(E) = \text{III}, \text{III}^* \\ \geq 5e + \beta_E + 1 & \text{en altre cas} \end{cases}$$
$$v(a_6') = \begin{cases} 6e + v(a_6) & \text{si } \text{tip}(E) = \text{II}, \text{I}_0^*, \text{II}^* \\ \geq 6e + \beta_E + 2 & \text{en altre cas.} \end{cases}$$

Per tant, dividint per $u = 2$, obtenim un model minimal amb $v(\Delta' u^{-12}) = v(\Delta)$. Això prova (iii).

Finalment, en les hipòtesis de (iv), torcem per χ i obtenim un model (1.4) amb:

$$v(a_4') = 4e + 2 + v(a_4).$$

Dividint per $u = \pi^{e+\alpha_E}$, tenim:

$$\begin{aligned} v(a_2' u^{-2}) &\geq 2 - \alpha_E \\ v(a_4' u^{-4}) &= v(a_4) + 2 - 4\alpha_E \\ v(a_6' u^{-6}) &\geq 5 + 2\beta_E - 6\alpha_E \end{aligned}$$

i de $v(\Delta' u^{-12}) = v(\Delta) + 6 - 12\alpha_E$ s'obté:

$$h_v = e + \alpha_E$$

Això acaba la demostració ∎

El teorema 1.1 descriu completament el comportament dels torcements quadràtics ramificats en $v \in \Sigma, p = 2$, quan E presenta un dels següents tipus: I_0, I_ν, III, IV, IV* o III*. En particular, se'n desprenen els corol·laris següents:

COROL·LARI 1.1.1.

En les hipòtesis del teorema 1.1, si E té reducció multiplicativa o bona reducció ordinària a v, aleshores:

$$tip(E^\chi) = I_\nu^*, \qquad h_v = 0.$$

DEMOSTRACIÓ:

Es conseqüència immediata de l'apartat (ii) del teorema.

COROL·LARI 1.1.2.

En les hipòtesis del teorema 1.1, si E té bona reducció supersingular a v, aleshores:

(a) *Si $2\delta(d) \geq 3v(b_2) + 4$, es té:*

$$tip(E^\chi) = I_\nu^*, \qquad h_v = \frac{1}{2} v(b_2).$$

(b) *Si $2\delta(d) < 3v(b_2) + 4$, posem $2\delta(d) = i + 6l$, $0 \leq i < 6$, llavors:*

$$tip(E^\chi) = II,\ I_0^*,\ II^*,\ \text{segons } i = 0, 2, 4 \text{ respectivament i } h_v = l.$$

DEMOSTRACIÓ:

És conseqüència immediata dels apartats (i) i (ii) del teorema 1.1, en imposar les condicions de supersingularitat ($v(b_2) > 0$, $v(b_6) = 0$) ∎

Anem ara a completar la descripció del comportament dels torcements quadràtics quan tip(E) = II, I_0^*, I_ν^* i II*, mitjançant els dos teoremes que seguidament enunciem i demostrem.

TEOREMA 1.2. *Suposem $p = 2$. Sigui $v \in \Sigma$ i χ un caràcter quadràtic, associat a $d \in K^*/K^{*2}$, ramificat a v. Sigui E una corba el·líptica sobre K, amb reducció a v de tipus II, I_0^* o II* i model v-minimal (1.3) satisfent: $\delta(d) = v(b_6) - \beta_E$ i $\delta(d) \leq v(b_2) - \alpha_E$. Llavors es té:*

(i) *Si $4\delta(d) \leq 3v(b_8) - 4\beta_E$ i $\delta(db_6) = 0$, posem:*

$$4\delta(d) + \beta_E = i + 6l, \qquad 0 \leq i < 6. \text{ Aleshores:}$$

tip(E^χ) = I_0, IV, IV segons $i = 0, 2, 4$ respectivament i $h_v = l$.*

(ii) *Si $4\delta(b_2b_6) \leq 4v(b_2) - v(b_8) + 2$, $4\delta(d) > 3v(b_8) - 4\beta_E$ i $4(\delta(db_6) - \delta(d)) \leq 4\beta_E - 3v(b_8) + 2$, posem:*

$$4\delta(d) + v(b_8) + 4\beta_E = i + 8l, \qquad 0 \leq i < 8. \text{ Aleshores:}$$

tip(E^χ) = III, III segons $i = 2, 6$ respectivament i $h_v = l$.*

(iii) *Si $4\delta(b_2b_6) > 4v(b_2) - v(b_8) + 2$, $4\delta(d) > 3v(b_8) - 4\beta_E$ i $\delta(db_6) - \delta(d) \leq 3(\delta(b_2b_6) - v(b_2) - 1) + \beta_E$, aleshores:*

$$\text{tip}(E^\chi) = I_\nu^*, \qquad h_v = \frac{1}{2}[\delta(d) + v(b_2) - \delta(b_2b_6)].$$

(iv) *En altre cas, posem:*

$$4\delta(d) - \delta(db_6) + \beta_E = i + 6l, \qquad 0 \leq i < 6. \text{ Aleshores:}$$

tip(E^χ) = II, I_0^*, II segons $i = 0, 2, 4$ respectivament i $h_v = l$.*

DEMOSTRACIÓ:

De $v(b_6 - a_3^2) = 2e + v(a_6)$ i $v(b_6) = \delta(d) + \beta_E$ es té: $\delta(b_6) = \delta(d)$.

En efecte, quan $v(d) = 1$ és clar, ja que $v(b_6) \equiv \delta(d) \pmod 2$. Si $v(d) = 0$, posem $\delta(d) = 2(e - k)$, aleshores $v(b_6 - a_3^2) = v(b_6) + 2k + 1$, i el resultat segueix de les propietats del discriminant.

Considerem el torcement quadràtic de E pel caràcter associat a b_6, que denotarem E^*. Sigui h_v^* el factor de correcció local de la fórmula dels discriminants minimals corresponent a aquest torcement.

Semblantment, denotem per E^{**} el torcement quadràtic de E^* pel caràcter associat a db_6, i sigui h_v^{**} el respectiu factor de correcció local. Aleshores, E^{**} i E^χ són K-isomorfes i, per tant,

$$\mathrm{tip}(E^{**}) = \mathrm{tip}(E^\chi).$$

A més, de les relacions:

$$12h_v^* = v(\mathcal{D}(E|K)) + 6\delta(d) - v(\mathcal{D}(E^*|K))$$
$$12h_v^{**} = v(\mathcal{D}(E^*|K)) + 6\delta(db_6) - v(\mathcal{D}(E^{**}|K))$$

s'obté:

$$h_v = h_v^* + h_v^{**} - \frac{1}{2}\delta(db_6). \tag{1.6}$$

Considerem el següent model de Weierstraß per a E^*:

$$y^2 + a_1^* xy + a_3^* y = x^3 + a_2^* x^2 \tag{1.7}$$

on

$$a_1^* = b_4 \qquad a_2^* = b_8$$
$$a_3^* = b_6^2 \qquad \Delta^* = (b_6)^6\Delta.$$

Aquest model s'obté de (1.4) en fer el canvi:

$$s = b_4, \qquad t = 4b_6^2, \qquad u = 2.$$

Tenim, doncs, $b_2^* = b_2 b_6$, $b_6^* = b_6^4$ i la desigualtat:

$$3v(b_2^*) - v(b_6^*) = 3v(b_2) - v(b_6) \geq 2\delta(d) - 2 > 2\delta(db_6) - 3 \tag{1.8}$$

ja que $\delta(db_6) \leq \delta(d)$.

Suposem, primer, $3v(b_8) \geq 4v(b_6)$. De (1.8) i la relació:

$$4b_8 = b_2 b_6 - b_4^2 \tag{1.9}$$

tenim: $3v(b_4) \geq 2v(b_6)$ i $v(\Delta) = 2v(b_6)$.

Posem $3\delta(d) + v(b_6) = i + 6l$, $0 \leq i < 6$. Llavors, $\mathrm{tip}(E^*) = \mathrm{I}_0$, IV, IV*, segons $i = 0, 2, 4$ respectivament i $h_v^* = l$.

En efecte, de $3\delta(d) + v(b_6) \equiv 4v(b_6) \pmod 6$, posem:

$$2v(b_6) = \frac{i}{2} + 3r.$$

Dividint el model (1.7) de E^* per $u = \pi^r$ obtenim:

$$v(a_3^* u^{-3}) = \frac{i}{2} \qquad v(a_1^* u^{-1}) \geq \frac{i}{6}$$
$$v(a_2^* u^{-2}) \geq \frac{i}{3} \qquad v(\Delta^* u^{-12}) = v(\Delta) - 2v(b_6) + 2i = 2i.$$

Suposem $3v(b_8) < 4v(b_6)$. Pel lema 1.2 tenim que $v(b_8) \not\equiv 0 \pmod 4$. Fem el següent canvi al model (1.7) de E^*:

$$s = \alpha - \frac{b_4}{2}, \qquad \text{on}$$

$\alpha = 0$ si $v(b_2 b_6) \equiv 1 \pmod 2$ i
$\alpha^2 \equiv \frac{b_2 b_6}{4} (\text{mod } \pi^{v(b_2 b_6) - \delta(b_2 b_6)})$ si $v(b_2 b_6) \equiv 0 \pmod 2$.

Obtenim, doncs, un nou model:

$$y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x,$$

on

$$a_1' = b_4 + 2s$$
$$a_2' = b_8 - b_4 s - s^2 = \frac{b_2 b_6}{4} - \alpha^2$$
$$a_3' = b_6^2$$
$$a_4' = -s b_6^2.$$

Observem que $2v(s) \geq v(b_8)$, amb igualtat quan $v(b_8) \equiv 0 \pmod 2$, ja que de la relació (1.9) es té:

$$2v(b_4) > v(b_8) \text{ i}$$

$$\delta(b_2 b_6) = \begin{cases} v(b_2 b_6) - v(b_8) + 1 & \text{si } v(b_8) \equiv 1 \pmod 2 \\ \leq v(b_2 b_6) - v(b_8) & \text{si } v(b_8) \equiv 0 \pmod 2. \end{cases} \tag{1.10}$$

D'aquí concloem:

$v(a_2') = v(b_8 - b_4 s - s^2) \geq v(b_8)$, desigualtat estricta quan $v(b_8) \equiv 0 \pmod 2$.

Si $4\delta(b_2 b_6) \leq 4v(b_2) - v(b_8) + 2$, en aquest cas per (1.10) hem de tenir necessàriament $v(b_8) \equiv 2 \pmod 4$. Posem:

$$4\delta(d) + v(b_8) = i + 8l, \qquad 0 \leq i < 8.$$

Aleshores, $\mathrm{tip}(E^*) = \mathrm{III}$, III^* segons $i = 2, 6$ respectivament i $h_v^* = l$.

En efecte, posem $2v(b_6) + \dfrac{v(b_8)}{2} = \dfrac{i}{2} + 4r$ i dividim el nou model de E^* per $u = \pi^r$. Així obtenim:

$$v(a_4' u^{-4}) = \frac{i}{2},\ v(a_2' u^{-2}) \geq v(b_2) - \frac{v(b_8) - i}{4} - \delta(b_2 b_6)$$
$$v(b_2' u^{-2}) = v(b_2^* u^{-2}) = v(b_2) - \frac{v(b_8) - i}{4}$$
$$v(b_6' u^{-6}) = v(b_6^* u^{-6}) = v(b_6) - \frac{3}{4}[v(b_8) - i]$$
$$\text{i } v(\Delta^* u^{-12}) = v(\Delta) - \frac{3v(b_8)}{2} + 3\frac{i}{2}.$$

Si $4\delta(b_2 b_6) \geq 4v(b_2) - v(b_8) + 3$, llavors:

$$\mathrm{tip}(E^*) = \mathrm{I}_\nu^*, \qquad h_v^* = \frac{1}{2}[\delta(d) + v(b_2) - \delta(b_2 b_6)].$$

En efecte, en aquest cas $v(a_2') = v(b_2 b_6) - \delta(b_2 b_6) + 1$. Dividim per $u = \pi^{\frac{1}{2}[v(a_2') - 1]}$ i obtenim:

$$v(a_2' u^{-2}) = 1$$
$$v(a_4' u^{-4}) \geq \frac{v(b_8)}{2} - 2v(b_2) + 2\delta(b_2 b_6),$$

amb igualtat quan $v(b_8) \equiv 0 \pmod 2$,

$$v(b_2^* u^{-2}) = \delta(b_2 b_6) \geq 2$$
$$v(b_6^* u^{-6}) = v(b_6) + 3[\delta(b_2 b_6) - v(b_2)] \geq v(b_6) - \frac{3}{4}[v(b_8) - 6]$$
$$v(\Delta^* u^{-12}) = v(\Delta) + 6\delta(b_2 b_6) - 6v(b_2).$$

A més, de $v(a_3' u^{-3}) - v(a_4' u^{-4}) = v(u) - v(s)$ deduïm (veure taula 1):

$$\nu = \begin{cases} 4v(b_6) - 3v(b_8) & \text{si } v(b_8) \equiv 1 \pmod 2 \\ v(b_8) + 4\delta(b_2 b_6) - 4v(b_2) - 4 & \text{si } v(b_8) \equiv 2 \pmod 4. \end{cases}$$

Finalment, torcem E^* per db_6.

Si $v(b_6^* u^{-6}) \geq \delta(db_6) + \beta_{E^*} + 1$, aleshores de (1.8): $v(b_2^* u^{-2}) \geq \delta(db_6) + \alpha_{E^*}$, amb desigualtat estricta quan $\mathrm{tip}(E^*) = \mathrm{I}_\nu^*$. Per l'apartat (iii) del teorema 1.1 tenim:

$$\mathrm{tip}(E^{**}) = \mathrm{tip}(E^*), \qquad h_v^{**} = \frac{1}{2}\delta(db_6)$$

i de (1.6) $h_v = h_v^*$.

Si $v(b_6^* u^{-6}) \leq \delta(db_6) + \beta_{E^*}$, de nou per (1.8) estem en les hipòtesis de (i) en el teorema 1.1. Per tant, posem:

$$v(b_6^* u^{-6}) + 2\delta(db_6) = i + 6l, \qquad 0 \leq i < 6.$$

Aleshores $\text{tip}(E^{**}) = \text{II}, \text{I}_0^*, \text{II}^*$, segons $i = 0, 2, 4$ respectivament i $h_v^{**} = l.$. De (1.6) i $h_v^* = \frac{1}{2}[\delta(d) - v(b_6)] + v(u)$ tenim $h_v = \frac{1}{6}[3\delta(d) + v(b_6) - \delta(db_6) - i]$.

Així obtenim, en cada cas, les condicions del teorema ∎

TEOREMA 1.3. *Suposem $p = 2$. Sigui $v \in \Sigma$ i E una corba el·líptica sobre K amb model v-minimal satisfent: $v(b_2) \leq 2e + 1$, $v(b_6) \geq 4$. Llavors es té:*

(i) *Si $v(b_6) < 3v(b_2)$, $3v(b_8) \geq 4v(b_6)$ i $\delta(b_2 b_6) = 0$ quan $v(b_8) < v(b_2) + v(b_6)$, posem:*

$$3v(b_2) + v(b_6) = i + 6l, \qquad 0 \leq i < 6. \text{ Aleshores:}$$

$tip(E^*) = I_0$, IV, IV^* segons $i = 0, 2, 4$ respectivament i $h_v^* = l$.

(ii) *Si $v(b_6) > 3v(b_2)$, $v(b_8) \geq 4v(b_2)$, aleshores:*

$h_v^* = v(b_2)$ i $tip(E^*) = I_0$, I_ν, segons $v(b_8) = 4v(b_2)$ o $v(b_8) > 4v(b_2)$, respectivament.

(iii) *Si $v(b_8) \equiv 2 \pmod 4$, $v(b_8) < \min(4v(b_2), v(b_6) - v(b_2))$, $3v(b_8) < 4v(b_6)$ i $4\delta(b_2 b_6) \leq 4v(b_6) - 3v(b_8) + 2$, posem:*

$$4v(b_2) + v(b_8) = i + 8l, \qquad 0 \leq i < 8. \text{ Aleshores:}$$

$tip(E^*) = III$, III^* segons $i = 2, 6$ respectivament i $h_v^* = l$.

(iv) *Si $\delta(b_2 b_6) \neq 0$, $v(b_8) < \min(4v(b_2), v(b_2) + v(b_6))$ i $4\delta(b_2 b_6) \geq 4v(b_6) - 3v(b_8) + 3$, posem:*

$$3v(b_2) + v(b_6) - \delta(b_2 b_6) = i + 6l, \qquad 0 \leq i < 6. \text{ Aleshores:}$$

$tip(E^*) = II$, I_0^*, II^*, segons $i = 0, 2, 4$, respectivament i $h_v^* = l$.

On E^* denota el torcement quadràtic de E pel caràcter associat a b_2 i h_v^*, el factor de correcció local de la fórmula dels discriminants minimals corresponent.

DEMOSTRACIÓ:

Considerem el següent model de Weierstraß per a E^*:

$$y^2 + a_1^* xy + a_3^* y = x^3 + a_6^* \tag{1.11}$$

on

$$a_1^* = b_2 \qquad a_6^* = b_2^2 b_8$$
$$a_3^* = b_2 b_4 \qquad \Delta^* = (b_2)^6 \Delta.$$

Aquest model s'obté de (1.4), en fer el canvi:

$$s = b_2, \qquad t = 4b_2 b_4, \qquad u = 2.$$

Suposem, primer, $v(b_6) > 3v(b_2)$, $v(b_8) \geq 4v(b_2)$; dividint el model (1.11) per $u = \pi^{v(b_2)}$ obtenim:

$$v(b_2^* u^{-2}) = 0 \qquad v(a_6^*) = v(b_8) - 4v(b_2)$$
$$v(b_6^* u^{-6}) = v(b_6) - 3v(b_2) \qquad v(\Delta^* u^{-12}) = v(\Delta) - 6v(b_2),$$

on $v(\Delta) = 6v(b_2)$ si $v(b_8) = 4v(b_2)$.

Això demostra l'asserció (ii).

Suposem $v(b_6) < 3v(b_2)$ i $v(b_8) \geq v(b_2) + v(b_6)$. De la relació:

$$4b_8 = b_2 b_6 - b_4^2 \tag{1.12}$$

tenim: $v(b_4) = v(b_2) + v(b_6)$ i $v(\Delta) = 2v(b_6)$. Posem:

$$3v(b_2) + v(b_6) = i + 6l, \qquad 0 \leq i < 6.$$

Dividint (1.11) per $u = \pi^l$ tenim:

$$v(a_3^* u^{-3}) = \frac{i}{2} \qquad v(b_2^* u^{-2}) \geq \frac{i}{3}$$
$$v(a_6^* u^{-6}) = v(b_8) - v(b_2) - v(b_6) + i \qquad v(\Delta^* u^{-12}) = 2i.$$

Per tant, $\mathrm{tip}(E^*) = \mathrm{I}_0$, IV, IV*, segons $i = 0, 2, 4$, respectivament.

Suposem, a partir d'ara, $v(b_8) < \min(4v(b_2), v(b_2) + v(b_6))$. Fem el següent canvi al model (1.11) de E^*:

$$t = \alpha - \frac{b_2 b_4}{2}, \text{ on}$$

$\alpha = 0$ si $v(b_2 b_6) \equiv 1 \pmod 2$ i

$\alpha^2 \equiv \frac{b_2^3 b_6}{4} (\mathrm{mod}\ \pi^{v(b_2^3 b_6) - \delta(b_2 b_6)})$ si $v(b_2 b_6) \equiv 0 \pmod 2$.

Obtenim, així, un nou model:

$$y^2 + a_1'xy + a_3'y = x^3 + a_4'x + a_6',$$

on

$$a_1' = b_2 \qquad a_4' = -tb_2$$
$$a_3' = b_2b_4 + 2t \qquad a_6' = b_2^2b_8 - tb_2b_4 - t^2 = \frac{b_2^3b_6}{4} - \alpha^2.$$

De $2v(b_4) > v(b_8)$ i del fet que:

$$\delta(b_2b_6) = \begin{cases} v(b_2b_6) - v(b_8) + 1 & \text{si } v(b_8) \equiv 1 \pmod 2 \\ \leq v(b_2b_6) - v(b_8) & \text{si } v(b_8) \equiv 0 \pmod 2 \end{cases}$$

tenim $v(a_6') = v(b_2^2b_8 - b_2b_4t - t^2) \geq 2v(b_2) + v(b_8)$, amb desigualtat estricta quan $v(b_8) \equiv 0 \pmod 2$.

Concloem, per tant:

$$2v(t) \geq 2v(b_2) + v(b_8),$$

amb igualtat quan $v(b_8) \equiv 0 \pmod 2$.

Si $3v(b_8) \geq 4v(b_6)$ i $\delta(b_2b_6) = 0$, de la desigualtat:

$$v(b_2) + v(b_6) < v(b_8) + 2e$$

i de la relació (1.12) tenim:

$$2v(b_4) = v(b_2) + v(b_6) < 4v(b_2)$$
$$v(a_3') = v(b_2) + v(b_4)$$
$$\text{i } v(\Delta') = v(\Delta) + 6v(b_2) = 2v(b_6) + 6v(b_2).$$

Posem $3v(b_2) + v(b_6) = i + 6l$, $0 \leq i < 6$.

Dividint el nou model de E^* per $u = \pi^l$ obtenim:

$$v(a_1'u^{-1}) \geq \frac{i}{6} \qquad v(a_4'u^{-4}) \geq \frac{4i}{6}$$
$$v(a_3'u^{-3}) = \frac{i}{2} \qquad v(a_6'u^{-6}) \geq i$$

i $v(\Delta'u^{-12}) = 2i$.

Això completa la demostració de l'asserció (i).

Si $4v(b_6) > 3v(b_8)$, $v(b_8) \equiv 2 \pmod 4$ i $4\delta(b_2b_6) \leq 4v(b_6) - 3v(b_8) + 2$, posem:

$$4v(b_2) + v(b_8) = i + 8l, \qquad 0 \leq i < 8.$$

Dividint per $u = \pi^l$ obtenim:

$$v(a'_4u^{-4}) = \frac{i}{2} \qquad v(b'_2u^{-2}) \geq \frac{2+i}{4}$$
$$v(a'_6u^{-6}) \geq \frac{3i-1}{4} \qquad v(b'_6u^{-6}) \geq \frac{2+3i}{4}$$

i $v(\Delta' u^{-12}) = v(\Delta) - \frac{3v(b_8)}{2} + \frac{3i}{2}$. D'aquí es desprèn l'asserció (iii) del teorema.

Finalment, si:

$$4\delta(b_2b_6) \geq 4v(b_6) - 3v(b_8) + 3, \qquad \delta(b_2b_6) \neq 0$$

posem: $3v(b_2) + v(b_6) - \delta(b_2b_6) = i + 6l$, $0 \leq i < 6$, i dividim per $u = \pi^l$, obtenint:

$$v(a'_6u^{-6}) = i+1 \qquad v(b'_6u^{-6}) \geq 2+i$$
$$v(a'_4u^{-4}) \geq \frac{3+4i}{6} \qquad v(b'_2u^{-2}) \geq \frac{2+i}{3}$$

i $v(\Delta' u^{-12}) = v(\Delta) - 2v(b_6) + 2\delta(b_2b_6) + 2i$.

Això prova la darrera asserció del teorema ∎

COROL·LARI 1.3. *Suposem $p = 2$. Sigui $v \in \Sigma$ i χ un caràcter quadràtic, associat a $d \in K^*/K^{*2}$, ramificat a v. Sigui E una corba el·líptica sobre K, amb reducció a v de tipus I_ν^* i model v-minimal (1.3) satisfent: $\delta(d) = v(b_2)$ i $\delta(d) \leq v(b_6) - 3$. Llavors es té:*

(a) *Si $\delta(db_2) = 0$, aleshores:*

$$tip(E^\chi) = tip(E^*) \text{ i } h_v = h_v^*.$$

(b) *Si $\delta(db_2) \cdot \delta(b_2b_6) \neq 0$, $4\delta(b_2b_6) \geq 4v(b_6) - 3v(b_8) + 3$, $4\delta(d) > \max(v(b_8), 4(v(b_8) - v(b_6)))$, aleshores:*

(b1) *Si $3\delta(db_2) \leq \min(3\delta(b_2b_6) - 3, 3\delta(d) - v(b_6) + \delta(b_2b_6) + \beta_{E^*} - 3\alpha_{E^*})$ es té:*

$$tip(E^\chi) = tip(E^*) \text{ i } h_v = h_v^*.$$

(b2) *Si $6\delta(db_2) \geq \max(9\delta(d) - 3v(b_6) + 9, 6\delta(d) - 2v(b_6) + 2\delta(b_2b_6) + 2[\beta_{E^*} - \alpha_{E^*} + 1])$ es té:*

$$tip(E^\chi) = I_\nu^*, \qquad h_v = \delta(d) - \frac{1}{2}\delta(db_2).$$

(b3) *Si $\delta(db_2) = \delta(b_2b_6)$ i $3\delta(d) \geq 2\delta(b_2b_6) + v(b_6) - \beta_{E^*} + 3\alpha_{E^*}$ aleshores:*

(b3.1) *Si $3v(b_8) \geq 4v(b_6)$ i $\delta(db_6) = 0$, posem:*

$$3\delta(d) + v(b_6) = i + 6l, \qquad 0 \leq i < 6. \text{ Es té:}$$

tip$(E^\chi) = I_0$, *IV*, *IV**, *segons* $i = 0, 2, 4$ *respectivament i* $h_v = l$.

(b3.2) *Si* $3v(b_8) < 4v(b_6)$, $4\delta(d) \geq 4\delta(b_2b_6) + v(b_8) - 2$ *i* $4\delta(db_6) \leq 4v(b_6) - 3v(b_8) + 2$, *posem:*

$$4[\delta(d) + \beta_{E^*}] + v(b_8) = i + 8l, \qquad 0 \leq i < 8. \text{ Es té:}$$

tip$(E^\chi) = III$, III^* *segons* $i = 2, 6$ *respectivament i* $h_v = l$.

(b3.3) *Si* $3v(b_8) < 4v(b_6)$, $4\delta(d) \leq 4\delta(b_2b_6) + v(b_8) - 3$ *i* $\delta(db_6) \leq v(b_6) + 3[\delta(b_2b_6) - \delta(d) - 1]$, *es té:*

$$tip(E^\chi) = I_\nu^*, \qquad h_v = \delta(d) - \frac{1}{2}\delta(db_2).$$

(b3.4) *En altre cas, posem:*

$$3\delta(d) + v(b_6) - \delta(db_6) = i + 6l, \qquad 0 \leq i < 6. \text{ Es té:}$$

tip$(E^\chi) = II$, I_0^*, II^* *segons* $i = 0, 2, 4$ *respectivament i* $h_v = l$.

(b4) *En altre cas, posem:*

$$3\delta(d) + v(b_6) - \delta(db_2) = i + 6l, \qquad 0 \leq i < 6. \text{ Es té:}$$

tip$(E^\chi) = II$, I_0^*, II^* *segons* $i = 0, 2, 4$, *respectivament i* $h_v = l$.

(c) *En altre cas:*

(c1) *Si* $2\delta(db_2) \geq 3\delta(d) - v(b_6) + 3$ *es té:*

$$tip(E^\chi) = I_\nu^*, \qquad h_v = \delta(d) - \frac{1}{2}\delta(db_2).$$

(c2) *Si* $4\delta(db_2) \leq \min(4v(b_6) - 3v(b_8) + 2, 4\delta(d) - v(b_8) + 2)$ *posem:*

$$4\delta(d) + v(b_8) = i + 8l,\ 0 \leq i < 8. \text{ Es té:}$$

tip$(E^\chi) = III$, III^* *segons* $i = 2, 6$ *respectivament i* $h_v = l$.

(c3) *En altre cas, com en (b4).*

DEMOSTRACIÓ:

De $v(b_2 - a_1^2) = 2e + 1$ i $v(b_2) = \delta(d)$ es té:

$$\delta(b_2) = \delta(d).$$

En efecte, quan $v(d) = 1$ és clar. Quan $v(d) = 0$ posem $\delta(d) = 2(e - k)$, aleshores $v(b_2a_1^2) = v(b_2) + 2k + 1$ i apliquem les propietats del discriminant.

Denotem per E^{**} el torcement quadràtic de E^* pel caràcter associat a db_2, i sigui h_v^{**} el corresponent factor de correcció local de la fórmula dels discriminants minimals. Aleshores:

$$\text{tip}(E^{**}) = \text{tip}(E^X) \text{ i, de les relacions:}$$

$$12h_v^* = v(\mathcal{D}(E|K)) + 6\delta(d) - v(\mathcal{D}(E^*|K))$$
$$12h_v^{**} = v(\mathcal{D}(E^*|K)) + 6\delta(db_2) - v(\mathcal{D}(E^{**}|K))$$

obtenim:

$$h_v = h_v^* + h_v^{**} - \frac{1}{2}\delta(db_2).$$

Es té també, (vegi's demostració del teorema 1.3)

$$h_v^* = v(u).$$

Per a $\delta(db_2) \neq 0$, obtenim les condicions del corol·lari, aplicant el teorema 1.2 al subcàs (b3) i el teorema 1.1 en els altres casos.

§3. Determinació de ν quan $\text{tip}(E^X) = \text{I}_\nu^*$. La fórmula dels conductors.

Suposem $p = 2$. Per a $v \in \Sigma$, sigui χ un caràcter quadràtic, associat a $d \in K^*/K^{*2}$, ramificat a v. Sigui E una corba el·líptica sobre K amb model v-minimal (1.3). Suposem que es satisfà alguna de les següents condicions:

A. $2\delta(d) \geq \max(3v(b_2) - v(b_6) + 3,\ 2(v(b_2) - \alpha_E + 1))$.
B. $\text{tip}(E) = \text{I}_{\nu'}^*$, ν' senar, $v(d) = 0$, $\delta(d) \leq \min(v(b_2) - 1,\ v(b_6) - 3)$.
C. $\text{tip}(E) = \text{II}, \text{I}_0^*, \text{II}^*$, $\delta(d) = v(b_6) - \beta_E$, $\delta(d) \leq v(b_2) - \alpha_E$, $4\delta(b_2b_6) > 4v(b_2) - v(b_8) + 2$, $4\delta(d) > 3v(b_8) - 4\beta_E$ i $\delta(db_6) - \delta(d) \leq 3(\delta(b_2b_6) - v(b_2) - 1) + \beta_E$.

Aleshores, pels teoremes 1.1 i 1.2 tenim:

$$\text{tip}(E^X) = \text{I}_\nu^*.$$

Anem a calcular ν, en cadascun dels casos A, B i C.

Considerem el següent model v-estàndard per a E^X:

$$y^2 + a_1^*xy + a_3^*y = x^3 + a_2^*x^2 + a_4^*x + a_6^* \tag{1.13}$$

($v(a_i^*)$ descrites a la taula 1).

Per un càlcul senzill es té:

$$v(b_8^*) = \nu + 4, \tag{1.14}$$

$$v(\Delta^*) = \nu + 2v(b_2^*) + 4, \text{ quan } v \geq 2v(b_2^*) - 2. \tag{1.15}$$

A.0 Suposem que es satisfà la condició A i $v(d) = 0$.

Existeix un model de Weierstraß minimal de E amb les propietats:

(1) $v(b_8) \not\equiv 0 \pmod 4$ quan: $4v(b_6) > 3v(b_8)$ i $4v(b_2) > v(b_8)$.
(2) $v(a_6) \equiv 1 \pmod 2$ quan: $v(b_6) \geq v(a_6) + \delta(d) - 1$ i $v(a_6) \leq 3v(b_2) - \delta(d)$.

En efecte, la propietat (1) és conseqüència immediata del lema 1.1, ja que $v(b_2) \leq \delta(d)$. Per a la propietat (2), suposem $v(b_6) \geq v(a_6)+\delta(d)-1$, $v(a_6) \leq 3v(b_2)-\delta(d)$ i $v(a_6) \equiv 0 \pmod 2$. Fent una traslladació per t, podem aconseguir: $v(a_6 - t^2) > v(a_6)$, i de $2v(a_3) \geq v(a_6) + \delta(d) - 1$ tenim:

$$v(a_6 - ta_3 - t^2) > v(a_6).$$

Aquest procés té un nombre finit de passos ja que $v(a_6)$ està acotat.

Notem que aquest nou model de E continua satisfent la condició A.

Obtenim un model minimal per a E^χ (vegi's demostració del teorema 1.1) dividint el model (1.5) de E^χ per $u = \pi^{v(a_1)+k}$, on $\delta(d) = 2(e-k)$. Tenim, doncs, $v(b_2^*) = v(b_2' u^{-2}) = \delta(d)$.

Sigui $r \in \mathcal{O}_v$ tal que:

$$b_8^* = b_8' u^{-8} + 3rb_6' u^{-6} + 3r^2 b_4' u^{-4} + r^3 b_2' u^{-2} + 3r^4.$$

Quan $r = 0$, posarem $v(r) = +\infty$.

A.0.1 Suposem $v(b_6) \geq 3v(b_2)$, $v(a_6) \geq 3v(b_2) - \delta(d) + 1$. Llavors,

$$\nu = \bar{v}(\Delta) - 6v(b_2) + 4(\delta(d) - 1).$$

En efecte, si $v(a_4) \geq 2v(b_2) - \delta(d) + 1$ tenim $\nu \geq 2v(b_2^*) - 2$ i aplicant (1.15) obtenim el resultat.

Si $v(a_4) < 2v(b_2) - \delta(d) + 1$ aleshores:

$$\begin{aligned} &v(a_4' u^{-4}) = v(a_4) + 2(\delta(d) - v(b_2)) \\ &v(a_3' u^{-3}) \geq v(a_4' u^{-4}) \\ &v(a_6' u^{-6}) \geq 2v(a_4' u^{-4}) - 1 \text{ i, per tant,} \end{aligned}$$

$$\nu = 2v(a_4' u^{-4}) - 4 = 2v(a_4) - 4v(b_2) + 4(\delta(d) - 1).$$

Finalment, el resultat s'obté de les relacions:

$$\begin{aligned} v(b_8) &= 2v(a_4) \\ v(\Delta) &= v(b_2^2 b_8). \end{aligned}$$

A.0.2 Suposem $v(b_6) < 3v(b_2)$, $v(b_6) \leq v(a_6) + \delta(d)$. Llavors,

$$\nu = v(\Delta) - 6v(b_2) + 4(\delta(d) - 1).$$

En efecte, de $v(a_6' u^{-6}) = v(b_6) - 3v(b_2) + 2\delta(d) + 1$ tenim:

$$v(a_6' u^{-6}) < \min(2v(a_3' u^{-3}), 2v(a_4' u^{-4}) - 1).$$

Per tant:

$$4v(r) = 2v(b_6) - 6v(b_2) + 4\delta(d).$$

Si $v(b_8) < 2(v(b_6) - v(b_2))$, llavors:

$$v(b_8^*) = v(b_8' u^{-8}) = v(b_8) - 4v(b_2) + 4\delta(d)$$

i $v(\Delta) = v(b_2^2 b_8)$.

Si $v(b_8) > 2(v(b_6) - v(b_2))$, llavors:

$$v(b_8^*) = 4v(r) \text{ i } v(\Delta) = v(b_6^2).$$

En els dos casos apliquem (1.14) per a obtenir el resultat. El cas $v(b_8) = 2(v(b_6) - v(b_2))$ s'evita en el nostre model minimal.

A.0.3 Suposem $v(b_6) \geq v(a_6) + \delta(d) - 1$, $v(b_8) \leq 2v(a_6) - 2v(b_2) + 2\delta(d) - 3$, aleshores:

$$\nu = v(\Delta) - 6v(b_2) + 4(\delta(d) - 1).$$

En efecte, de $v(a_6' u^{-6}) \geq v(a_6) - 3v(b_2) + 3\delta(d)$ tenim:

$$4v(r) \geq 2v(a_6) - 6v(b_2) + 6\delta(d) - 2$$

i $v(b_8^*) = v(b_8' u^{-8})$, amb $v(\Delta) = v(b_2^2 b_8)$.

A.0.4 Suposem $v(b_6) > v(a_6) + \delta(d) - 1$, $v(a_6) \leq 3v(b_2) - \delta(d)$ i $v(b_8) > 2v(a_6) - 2v(b_2) + 2\delta(d) - 3$, aleshores:

$$\nu = 2v(a_6) - 6v(b_2) + 6(\delta(d) - 1).$$

En efecte, de $v(a_6' u^{-6}) = v(a_6) - 3v(b_2) + 3\delta(d)$ i $v(b_8) = v(a_1^2 a_6 - a_4^2)$ tenim:

$$v(a_6' u^{-6}) < \min(2v(a_3' u^{-3}),\ 2v(a_4' u^{-4}) - 1)$$

i, per tant,

$$4v(r) = 2v(a_6) - 6v(b_2) + 6\delta(d) - 2,$$

on en el nostre model $v(a_6) \equiv 1 \pmod 2$. Finalment es té:

$$v(b_8^*) = 4v(r).$$

A.0.5 Suposem $v(b_6) = v(a_6) + \delta(d) - 1$, $v(a_6) \leq 3v(b_2) - \delta(d)$, $v(b_8) > 2v(a_6) - 2v(b_2) + 2\delta(d) - 3$, aleshores:

Si $2\delta(db_6) < 2v(b_6) - 2v(b_2) - v(b_8) + 2\delta(d)$:

$$\nu = v(b_8) - 4v(b_2) + 4(\delta(d) - 1).$$

Si $2\delta(db_6) \geq 2v(b_6) - 2v(b_2) - v(b_8) + 2\delta(d)$:

$$\nu = v(\Delta) - 6v(b_2) + 2(3\delta(d) - \delta(db_6) - 2).$$

En efecte, la igualtat $v(b_6) = v(a_6) + \delta(d) - 1$ implica $v(a_6) \equiv 1 \pmod 2$ i, com en el subcàs anterior, es té $v(b_8) = v(a_1^2 a_6 - a_4^2)$.

Considerem el model (1.5) per a E^χ, on ara escollim $\alpha \in \mathcal{O}_v$ tal que:

$$d \equiv \alpha^2 (\text{mod } \pi^{2e-\delta(d)+1})$$
$$db_6 \equiv (a_3\alpha)^2 (\text{mod } \pi^{2e-\delta(db_6)+v(db_6)}).$$

Tenim, doncs,

$$v(a_6') = v(16d^2(db_6 - (a_3\alpha)^2)) = v(b_6) - \delta(db_6) + 6e + 1,$$

si $\delta(db_6) \neq 0$. Per tant,

$$4v(r) \geq 2v(b_6) - 6v(b_2) + 6\delta(d) - 2\delta(db_6), \text{ si } \delta(db_6) \neq 0$$

i d'aquí, si $2\delta(db_6) < 2v(b_6) - 2v(b_2) - v(b_8) + 2\delta(d)$ es té: $v(b_8^*) = v(b_8' u^{-8})$.

Si $2\delta(db_6) \geq 2v(b_6) - 2v(b_2) - v(b_8) + 2\delta(d)$, tenim

$$\delta(db_6) \neq 0 \text{ i } v(a_6' u^{-6}) < \min(2v(a_3' u^{-3}), 2v(a_4' u^{-4}) - 1).$$

Per tant, $4v(r) = 2v(b_6) - 6v(b_2) + 6\delta(d) - 2\delta(db_6)$ i $v(b_8^*) = 4v(r)$.

Finalment, de $\delta(db_6) \leq \delta(d)$ tenim $v(b_8) > 2(v(b_6) - v(b_2))$ i d'aquí $v(\Delta) = 2v(b_6)$.

A la taula 2, donem un recull de tots els resultats en el cas A.0.

A.1 Suposem que es satisfà la condició A i $v(d) = 1$.

Escollim un model minimal de E que satisfaci: $v(b_8) \not\equiv 0 \pmod 4$ si: $4v(b_6) > 3v(b_8)$ i $4v(b_2) > v(b_8)$. L'existència d'un tal model és immediata a partir del lema 1.1.

Obtenim un model minimal per a E^χ (vegi's demostració del teorema 1.1) dividint el model (1.4) de E^χ per $u = \pi^{v(a_1)}$. Sigui $r \in \mathcal{O}_v$ com en el cas A.0.

A.1.1 Suposem $v(b_6) \geq 3v(b_2)$, aleshores:

$$\nu = v(\Delta) - 6v(b_2) + 4(\delta(d) - 1).$$

En efecte, en aquest cas tenim $\nu \geq 2v(b_2^*) - 2$, on $v(b_2^*) = \delta(d)$ i aplicant (1.15) obtenim el resultat.

A.1.2 Suposem $v(b_6) < 3v(b_2)$, $v(b_6) \equiv 0 \pmod 2$. Aleshores:

$$\nu = v(\Delta) - 6v(b_2) + 4(\delta(d) - 1).$$

Taula 2

<table>
<tr><td colspan="4">$2\delta(d) \geq \max(3v(b_2) - v(b_6) + 3,\quad 2(v(b_2) - \alpha_E + 1)),\qquad v(d) = 0$</td><td>$\nu(E^x)$</td></tr>
<tr><td rowspan="2">$v(b_6) \geq 3v(b_2)$</td><td colspan="3">$\delta(d) \geq 3v(b_2) - v(a_6) + 1$ o
$2\delta(d) \geq v(b_8) + 2v(b_2) - 2v(a_6) + 3$</td><td>$v(\Delta) - 6v(b_2) + 4(\delta(d) - 1)$</td></tr>
<tr><td colspan="3">$2\delta(d) < \min(v(b_8) + 2v(b_2) - 2v(a_6) + 3,\quad 2(3v(b_2) - v(a_6) + 1))$</td><td>$2v(a_6) - 6v(b_2) + 6(\delta(d) - 1)$</td></tr>
<tr><td rowspan="4">$v(b_6) < 3v(b_2)$</td><td colspan="3">$\delta(d) > v(b_6) - v(a_6) + 1$ o
$2\delta(d) \geq v(b_8) + 2v(b_2) - 2v(a_6) + 3$</td><td>$v(\Delta) - 6v(b_2) + 4(\delta(d) - 1)$</td></tr>
<tr><td rowspan="3">$2\delta(d) < v(b_8) + 2v(b_2) - 2v(a_6) + 3$</td><td colspan="2">$\delta(d) < v(b_6) - v(a_6) + 1$</td><td>$2v(a_6) - 6v(b_2) + 6(\delta(d) - 1)$</td></tr>
<tr><td rowspan="2">$\delta(d) = v(b_6) - v(a_6) + 1$</td><td>$2(\delta(db_6) - \delta(d)) < 2(v(b_6) - v(b_2)) + v(b_8)$</td><td>$v(b_8) - 4v(b_2) + 4(\delta(d) - 1)$</td></tr>
<tr><td>$2(\delta(db_6) - \delta(d)) \geq 2(v(b_6) - v(b_2)) + v(b_8)$</td><td>$v(\Delta) - 6v(b_2) + 2(3\delta(d) - \delta(db_6) - 2)$</td></tr>
</table>

En efecte, de $v(a_6u^{-6}) = v(b_6) - 3v(b_2) + 4e + 3$ tenim:

$$4v(r) \geq 2v(b_6) - 6v(b_2) + 4\delta(d).$$

Si $v(b_8) < 2v(b_6) - 2v(b_2)$ aleshores $v(b_8^*) = v(b_8'u^{-8})$ i $v(\Delta) = v(b_2^2b_8)$.
Si $v(b_8) > 2v(b_6) - 2v(b_2)$ aleshores de $v(a_6'u^{-6}) < 2v(a_4'u^{-4}) - 1$ tenim $4v(r) = 2v(b_6) - 6v(b_2) + 4\delta(d)$ i $v(b_8^*) = 4v(r)$, amb $v(\Delta) = v(b_6^2)$.
El cas $v(b_8) = 2v(b_6) - 2v(b_2)$ no es dóna en el nostre model.
A.1.3 Suposem $v(b_6) < 3v(b_2)$, $v(b_6) \equiv 1 \pmod 2$. Aleshores:
Si $2\delta(db_6) < 2v(b_6) - 2v(b_2) - v(b_8) + 2\delta(d)$:

$$\nu = v(b_8) - 4v(b_2) + 4(\delta(d) - 1).$$

Si $2\delta(db_6) \geq 2v(b_6) - 2v(b_2) - v(b_8) + 2\delta(d)$:

$$\nu = v(\Delta) - 6v(b_2) + 2(3\delta(d) - \delta(db_6) - 2).$$

En efecte, fem el següent canvi al model (1.4) de $E^\chi : t \equiv 4d\alpha$, on

$$db_6 \equiv \alpha^2 (\text{mod } \pi^{2e-\delta(db_6)+v(db_6)}).$$

Tenim, doncs:

$$v((a_6' - t^2)u^{-6}) = v(b_6) - 3v(b_2) - \delta(db_6) + 6e + 4, \text{ si } \delta(db_6) \neq 0.$$

A partir d'aquí es procedeix com en el subcàs A.0.5.
B. Suposem que es satisfà la condició B. Aleshores:

$$\begin{aligned} &\text{Si } 2\delta(d) < \nu' + 3: && \nu = \nu' \\ &\text{Si } 2\delta(d) \geq \nu' + 3: && \nu = 2(\nu' - \delta(d) + 1). \end{aligned}$$

En efecte, prenem el model v-estàndard per a E (vegi's taula 1). Obtenim un model minimal per a E^χ (vegi's demostració del teorema 1.1) dividint el model (1.5) de E^χ per $u = 2$. Sigui $r \in \mathcal{O}_v$ com en els casos anteriors. Tenim:

$$\begin{aligned} &v(a_6'u^{-6}) = v(b_6) - \delta(d) + 1 \\ &v(a_4'u^{-4}) \geq v(a_3'u^{-3}) + 1 \\ &v(a_6'u^{-6}) < 2v(a_3'u^{-3}), \text{ per tant,} \end{aligned}$$

$$\begin{aligned} &4v(r) = 2v(b_6) - 2\delta(d) \qquad \text{i} \\ &v(b_8'u^{-8}) = v(b_8) = v(b_6) + 1. \end{aligned}$$

Si $v(b_6) > 2\delta(d)$ llavors $v(b_8^*) = v(b_8)$.
Si $v(b_6) \leq 2\delta(d)$ llavors $v(b_8^*) = 4v(r)$.

C. Suposem que es satisfà la condició C.

Sigui E^* el torcement de E pel caràcter associat a b_6. Hem provat a la demostració del teorema 1.2 que $\mathrm{tip}(E^*) = \mathrm{I}^*_{\nu'}$, amb model v-estàndard obtingut en transformar el model (1.7) per $s = \dfrac{\alpha}{2}$ i $u = \pi^{\frac{1}{2}(v(b_2b_6)-\delta(b_2b_6))}$ i ν' donada per:

$$\nu' = \begin{cases} 4v(b_6) - 3v(b_8) & \text{si } v(b_8) \equiv 1 \pmod 2 \\ v(b_8) - 4v(b_2) + 4(\delta(b_2b_6) - 1) & \text{si } v(b_8) \equiv 2 \pmod 4. \end{cases}$$

Sigui E^{**} el torcement de E^* pel caràcter associat a db_6. Tenim, doncs, $\nu(E^{\chi}) = \nu(E^{**})$.

C.1 Suposem $v(b_8) \equiv 1 \pmod 2$. Aleshores:

Si $\delta(db_6) - 4\delta(d) < 4\beta_E - 3v(b_8) + 3$: $\quad \nu = 4\delta(d) - 3v(b_8) + 4\beta_E$.
Si $\delta(db_6) - 4\delta(d) \geq 4\beta_E - 3v(b_8) + 3$: $\quad \nu = 2(4\delta(d) - 3v(b_8) - \delta(db_6) + 4\beta_E + 1)$.

En efecte, només cal aplicar el resultat del cas B a E^{**}.

C.2 Suposem $v(b_8) \equiv 2 \pmod 4$. Aleshores:

Si $\delta(db_6) - \delta(d) < \delta(b_2b_6) - v(b_2) - \dfrac{v(b_8)}{2} + \beta_E$:

$$\nu = v(b_8) - 4v(b_2) + 4(\delta(b_2b_6) - 1).$$

Si $\delta(db_6) - \delta(d) > \delta(b_2b_6) - v(b_2) - \dfrac{v(b_8)}{2} + \beta_E$:

$$\nu = 2\delta(d) + 6\delta(b_2b_6) - 2\delta(db_6) - 6v(b_2) + 2\beta_E - 4.$$

En efecte, considerem el model v-estàndard de E^*. Obtenim un model minimal per a E^{χ} dividint el model (1.5) de E^{**} per $u = 2$. Sigui $r \in \mathcal{O}_v$ com abans, és a dir, la traslladó de x que ens passa de l'anterior model minimal al model v-estàndard de E^{χ}. Llavors tenim:

$$v(a_6'u^{-6}) = v(b_6) - 3v(b_2) + 3\delta(b_2b_6) - \delta(db_6) + 1$$
$$\text{i } 4v(r) \geq 2v(b_6) - 6v(b_2) + 6\delta(b_2b_6) - 2\delta(db_6).$$

Si $v(b_8'u^{-8}) < 2v(b_6) - 6v(b_2) + 6\delta(b_2b_6) - 2\delta(db_6)$ aleshores $v(b_8^*) = v(b_8'u^{-8})$.
Si $v(b_8'u^{-8}) \geq 2v(b_6) - 6v(b_2) + 6\delta(b_2b_6) - 2\delta(db_6)$ aleshores $v(a_6'u^{-6}) < 2v(a_4'u^{-4}) - 1$, $4v(r) = 2v(b_6) - 6v(b_2) + 6\delta(b_2b_6) - 2\delta(db_6)$ i $v(b_8^*) = 4v(r)$.

REMARQUES:

(1.1) Si $\text{tip}(E) = \text{I}_0$, I_ν, III, IV, III* o IV* i es satisfà la condició A, aleshores:

$$\nu = v(\Delta) - 6v(b_2) + 4(\delta(d) - 1)$$

aquesta igualtat surt clarament en aplicar A.0, A.1 a cadascun dels tipus esmentats.

(1.2) El coneixement de ν en els casos A, B i C, ens permet calcular-la també en tots els altres casos, els quals es poden presentar quan $\text{tip}(E) = \text{I}^*_{\nu'}$ i $\delta(d) \leq v(b_2)$, $\delta(d) \leq v(b_6) - 3$. Un camí és:

(i) Si $\delta(d) = v(b_2)$, apliquem el teorema 1.3, per a classificar E^* i tot seguit els algorismes A, B o C al torcement de E^* per db_2.

(ii) Si $\delta(d) < v(b_2)$ (i ν' és parell), donem dues opcions:

(a) Prenem un model minimal de E que compleixi les propietats següents:
(1) $v(b_8) \not\equiv 0 \pmod 4$ quan: $4v(b_6) > 3v(b_8)$ i $4v(b_2) > v(b_8)$.
(2) $v(b_6) \neq 3v(b_2)$ quan $v(b_8) \geq 4v(b_2)$.
Un tal model sempre existeix, pels lemes 1.1 i 1.2, ja que $v(b_2) \leq 2e + 1$. Ara estem en condicions d'aplicar el teorema 1.3 i procedir com en (i).

(b) Considerem el model v-estàndard de E. És un càlcul senzill veure que, si $2\delta(d) \neq 2v(b_6) - v(b_8)$ es té:

$$\begin{array}{ll} \nu = 2(v(b_6) - \delta(d) - 2) & \text{quan } 2\delta(d) > \max(2v(b_6) - v(b_8), \\ & \quad 2(v(b_6) - v(a_6) + 1)) \\ \nu = \nu' & \text{en altre cas.} \end{array}$$

En particular, quan $2\delta(d) < \nu' + 4$ tenim $\nu = \nu'$.

Finalment, en el cas $2\delta(d) = 2v(b_6) - v(b_8)$ procedim com en (a).

La fórmula dels conductors.

Sigui $E|K$ una corba el·líptica definida sobre K amb discriminant minimal $\mathcal{D}(E|K)$ i conductor geomètric $\mathcal{N}(E|K)$ (cf. [Og3], [STN]). Per un caràcter quadràtic χ, considerem la corba el·líptica E^χ amb discriminant minimal $\mathcal{D}(E^\chi|K)$ i conductor geomètric $\mathcal{N}(E^\chi|K)$.

Donat $v \in \Sigma$ tenim,

$$f_v = v(\mathcal{D}(E|K) + 1 - m_v$$
$$f_v^\chi = v(\mathcal{D}(E^\chi|K) + 1 - m_v^\chi.$$

On notem $f_v = v(\mathcal{N}(E|K))$, $f_v^\chi = v(\mathcal{N}(E^\chi|K))$ i m_v, m_v^χ denoten el nombre de components irreductibles (llevat de multiplicitats) de la fibra especial del model v-regular, v-minimal de E, E^χ, respectivament.

A partir de la relació entre els discriminants minimals d'ambdues corbes, hom pot donar, doncs, una relació entre els conductors geomètrics respectius que, localment, es podrà escriure així:

$$f_v^\chi - f_v = 6v(\mathcal{D}(X)) + m_v - m_v^\chi - 12h_v.$$

EXEMPLES:

1) Quan la fórmula de Silverman (1.1) sigui certa a v (és a dir, per $h_v = 0$) tindrem:
$$f_v^\chi - f_v = 6v(\mathcal{D}(X)) + m_v - m_v^\chi.$$

2) Si χ és no-ramificat a v, aleshores:
$$f_v^\chi = f_v.$$

3) Si $p \neq 2$ i χ és ramificat a v, aleshores de la proposició de la pàg. 15 tenim: $f_v^\chi - f_v = 0$, llevat quan $\mathrm{tip}(E) = \mathrm{I}_0, \mathrm{I}_\nu, \mathrm{I}_0^*, \mathrm{I}_\nu^*$. En aquest cas $f_v^\chi - f_v = 2, 1, -2, -1$, respectivament.

4) Suposem $p = 2$ i χ ramificat a v. Obtenim $f_v^\chi - f_v$ dels teoremes 1.1, 1.2, 1.3, el Corol·lari 1.3 i el càlcul de m_v^χ (quan $\mathrm{tip}(E^\chi) = \mathrm{I}_\nu^*$).

(4.1) En les hipòtesis del teorema 1.1 (i) tenim:
$$f_v^\chi - f_v = 2\delta(d) + m_v - 2v(b_6) - 1.$$

(4.2) En les hipòtesis del teorema 1.1 (ii), quan $\mathrm{tip}(E) = \mathrm{I}_0, \mathrm{I}_\nu$, III, IV, III*, IV*, tenim:
$$f_v^\chi - f_v = 2\delta(d) + m_v - v(\Delta) - 1.$$

(4.3) En les hipòtesis del teorema 1.1 (iii), amb $2\delta(d) < \nu + 4$ si $\mathrm{tip}(E) = \mathrm{I}_\nu^*$, tenim:
$$f_v^\chi - f_v = 0.$$

(4.4) En les hipòtesis del teorema 1.1 (iv) tenim:
$$f_v^\chi - f_v = 0.$$

(4.5) En les hipòtesis del teorema 1.2 (i) tenim:
$$f_v^\chi - f_v = \begin{cases} -2\delta(d) & \text{si } i = 0 \\ -2\delta(d) + 2 & \text{si } i = 2, 4. \end{cases}$$

(4.6) En les hipòtesis del teorema 1.2 (ii) tenim:
$$f_v^\chi - f_v = 2 - 4\beta_E - \frac{3}{2}v(b_8).$$

(4.7) En les hipòtesis del teorema 1.2 (iii) tenim:

$$f_v^\chi - f_v = 6\delta(b_2 b_6) + 2\beta_E - 6v(b_2) - \nu - 4$$

on ν ve donada per C.1, C.2 (vegi's pàg. 37).

(4.8) En les hipòtesis del teorema 1.2 (iv) tenim:

$$f_v^\chi - f_v = 2(\delta(db_6) - \delta(d)).$$

En les taules que segueixen, explicitem per a $v \in \Sigma$, $p = 2$, $e = 1$, per a un caràcter quadràtic χ ramificat a v -amb $v(d) = 0$ a la taula 3 i amb $v(d) = 1$ a la taula 4- i per a una corba el·líptica E amb model v-minimal (1.3), el tipus de reducció de E^χ així com les relacions locals entre els discriminants minimals i els conductors geomètrics de E i E^χ.

Taula 3

$tip(E)$				$tip(E^x)$	h_v	$v(\mathcal{D}(E^x)) - v(\mathcal{D}(E))$	$f_v^x - f_v$
I_0	$v(b_2) = 0$			I_ν^* $(\nu=4)$	0	12	4
	$v(b_2) > 0$			II^*	0	12	4
I_ν				$I_{\nu'}^*$ $(\nu'=\nu+4)$	0	12	3
II	$v(b_6) > 2$			II	1	0	0
	$v(b_6) = 2$	$\delta(db_6) = 2$		II	1	0	0
		$\delta(db_6) = 0$	$v(b_8) = 2$	III	1	0	-1
			$v(b_8) > 2$	IV	1	0	-2
III	$v(b_6) = 2$			II	1	0	1
	$v(b_6) > 2$			III	1	0	0
IV				II	1	0	2
I_0^*	$v(b_6) > 4$			I_0^*	1	0	0
	$v(b_6) = 4$	$\delta(db_6) = 2$		I_0^*	1	0	0
		$\delta(db_6) = 0$	$v(b_8) = 5$	I_ν^* $(\nu=1)$	1	0	-1
			$v(b_8) > 5$	IV^*	1	0	-2
I_ν^*	$v(b_6) = 4$			I_0^*	1	0	ν
	$v(b_6) > 4$	$v(b_2) > 2$		$I_{\nu'}^*$ $(\nu'=\nu)$	1	0	0
		$v(b_2) = 2$	$\delta(db_2) = 2$	$I_{\nu'}^*$ $(\nu'=v(\Delta)-8)$	1	0	$\nu - v(\Delta) + 8$
			$\delta(db_2) = 0$ $v(b_8) = 6$	III^*	1	0	$\nu - 3$
			$v(b_8) = 7$	II^*	1	0	$\nu - 4$
			$v(b_8) = 8$	I_0	2	-12	$\nu - 8$
			$v(b_8) > 8$	$I_{\nu'}$ $(\nu'=v(\Delta)-12)$	2	-12	$\nu - v(\Delta) + 5$

Taula 3 (cont.)

$tip(E)$				$tip(E^{\chi})$	h_v	$v(\mathcal{D}(E^{\chi})) - v(\mathcal{D}(E))$	$f_v^{\chi} - f_v$
IV^*				I_0^*	1	0	2
III^*	$v(b_2) = 2$			I_ν^{*} $(\nu=2)$	1	0	1
	$v(b_2) > 2$			III^*	1	0	0
II^*	$v(b_2) = 2$			I_ν^{*} $(\nu=3)$	1	0	1
	$v(b_2) > 2$	$v(b_6) > 6$		II^*	1	0	0
		$v(b_6) = 6$	$\delta(db_6) = 2$	II^*	1	0	0
			$\delta(db_6) = 0$	I_0	2	-12	-4

Taula 4

$tip(E)$					$tip(E^\chi)$	h_v	$v(\mathcal{D}(E^\chi)/\mathcal{D}(E))$	$f_v^\chi - f_v$
I_0	$v(b_2)=0$				I_ν^* $(\nu=8)$	0	18	6
	$v(b_2)>0$				II	1	6	6
I_ν					$I_{\nu'}^*$ $(\nu'=\nu+8)$	0	18	5
II	$v(b_6)=2$				I_0^*	1	6	2
	$v(b_6)=3$	$v(b_2)=2$			I_ν^* $(\nu=v(b_8))$	1	6	$2-v(b_8)$
		$v(b_2)>2$	$v(b_8)=2$		III^*	1	6	-1
			$v(b_8)>2$	$\delta(db_6)=2$	II^*	1	6	-2
				$\delta(db_6)=0$	I_0	2	-6	-6
III	$v(b_6)=2$				I_0^*	1	6	3
	$v(b_6)>2$	$v(b_2)=2$			I_ν^* $(\nu=2)$	1	6	1
		$v(b_2)>2$			III^*	1	6	0
IV					I_0^*	1	6	4
IV^*	$v(b_2)=2$				I_ν^* $(\nu=4)$	1	6	4
	$v(b_2)>2$				II^*	1	6	4
III^*	$v(b_2)=2$				I_ν^* $(\nu=6)$	1	6	3
	$v(b_2)>2$	$v(b_6)=6$			II	2	-6	1
		$v(b_6)>6$			III	2	-6	0
II^*	$v(b_2)=2$				I_ν^* $(\nu=7)$	1	6	3
	$v(b_2)>2$	$v(b_6)=6$			II	2	-6	2
		$v(b_6)=7$	$\delta(db_6)=2$		I_0^*	2	-6	-2
			$\delta(db_6)=0$	$v(b_8)=9$	I_ν^* $(\nu=1)$	2	-6	-3
				$v(b_8)>9$	IV^*	2	-6	-4

Taula 4(cont.)

$tip(E)$					$tip(E^{\chi})$	h_v	$v(\mathcal{D}(E^{\chi})/\mathcal{D}(E))$	$f_v^{\chi} - f_v$
I_0^*	$v(b_2) = 2$				I_ν^* $(\nu = v(\Delta) - 4)$	1	6	$10 - v(\Delta)$
	$v(b_2) > 2$	$v(b_6) = 4$			II^*	1	6	2
		$v(b_6) = 5$	$v(b_8) = 5$		I_ν^* $(\nu = 5)$	1	6	1
			$v(b_8) > 5$	$\delta(db_6) = 2$	II	2	-6	-2
				$\delta(db_6) = 0$, $v(b_8) = 6$	III	3	-18	-15
				$\delta(db_6) = 0$, $v(b_8) > 6$	IV	2	-6	-4
I_ν^*	$v(b_2) = 2$				$I_{\nu'}^*$ $(\nu' = v(\Delta) - 4)$	1	6	$\nu + 10 - v(\Delta)$
	$v(b_2) = 3$	$v(b_6) = 4$			II^*	1	6	$\nu + 2$
		$v(b_6) = 6$	$v(b_8) = 6$	$\delta(db_2) = 0$	II	2	-6	$\nu - 2$
				$\delta(db_2) = 2$	III	2	-6	$\nu - 3$
			$v(b_8) = 7$		II	2	-6	$\nu - 2$
		$v(b_6) = 7$	$v(b_8) = 6$		III	2	-6	$\nu - 3$
			$v(b_8) = 9$	$\delta(db_2) = 0$	I_0^*	2	-6	$\nu - 6$
				$\delta(db_2) = 2$, $\delta(db_6) = 0$	$I_{\nu'}^*$ $(\nu' = 1)$	2	-6	$\nu - 7$
				$\delta(db_2) = 2$, $\delta(db_6) = 2$	I_0^*	2	-6	$\nu - 6$
			$v(b_8) > 9$	$\delta(db_2) = 0$	IV^*	2	-6	$\nu - 8$
				$\delta(db_2) = 2$	I_0^*	2	-6	$\nu - 6$
		$v(b_6) > 7$	$v(b_8) = 9$		I_0^*	2	-6	$\nu - 6$
			$v(b_8) \neq 9$	$\delta(db_2) = 2$	$I_{\nu'}^*$ $(\nu' = v(\Delta) - 14)$	2	-6	$\nu + 8 - v(\Delta)$
				$\delta(db_2) = 0$, $v(b_8) = 6$	III	2	-6	$\nu - 3$
				$\delta(db_2) = 0$, $v(b_8) = 10$	III^*	2	-6	$\nu - 9$
				$\delta(db_2) = 0$, $v(b_8) = 11$	II^*	2	-6	$\nu - 10$
				$\delta(db_2) = 0$, $v(b_8) = 12$	I_0	3	-18	$\nu - 14$
				$\delta(db_2) = 0$, $v(b_8) > 12$	$I_{\nu'}^*$ $(\nu' = v(\Delta) - 18)$	3	-18	$\nu + 5 - v(\Delta)$

CAPÍTOL II. CORBES EL·LÍPTIQUES D'INVARIANT j FIXAT I BONA REDUCCIÓ.

Sigui K un cos de nombres. Podem descriure el conjunt de totes les corbes el·líptiques definides sobre K, de la següent manera:

Per a cada $j \in K$, $j \neq 0, 1728$, considerem la corba el·líptica E_j, donada per la següent equació afí de Weierstraß:

$$y^2 = x^3 - \frac{27j}{j-1728}x - \frac{54j}{j-1728}$$

amb $j(E_j) = j$. Sigui $Ell(j)$ el conjunt de totes les corbes el·líptiques que tenen el mateix invariant j. Aleshores $Ell(j) = \text{Twist}(E_j)$ és un espai homogeni principal sobre $H^1(G_K, \text{Aut}(E_j)) \cong H^1(G_K, \mathbb{Z}/2\mathbb{Z}) \cong K^*/K^{*^2}$. És a dir, cada corba el·líptica sobre K (amb $j \neq 0, 1728$) és un torcement quadràtic d'alguna E_j i ve, per tant, parametritzada per la parella: $(j \in K, d \in K^*/K^{*^2})$.

Considerem, ara, el següent problema:

Sigui $Ell_S = \{\text{corbes el·líptiques sobre } K \text{ amb bona reducció fora de } S\}$

on S és un conjunt finit de primers finits de K. Com es pot descriure el conjunt Ell_S mitjançant els paràmetres (j, d)?.

És molt senzill veure que el conjunt de corbes de Ell_S amb invariant j fixat és també un espai homogeni principal, però, sobre la cohomologia no-ramificada fora de S. Tenim, doncs, que el conjunt $Ell_S \cap Ell(j)$ és buit, o bé, si $E \in Ell_S \cap Ell(j)$, tots els elements restants són torcements de E per caràcters quadràtics no-ramificats fora de S. Per tant, el problema plantejat es redueix a detallar el següent conjunt:

$$J_S = \{j \in K : \text{ existeix una corba el·líptica } E|K \text{ amb bona reducció fora de } S \text{ i } j(E) = j\}.$$

El procediment que utilitzem per a la descripció de J_S comprèn un estudi previ del problema en el cas local.

Observem que, fixat $v \in \Sigma$, podem descriure el conjunt de corbes el·líptiques sobre el cos K_v com abans. El mateix podem fer amb el conjunt de corbes el·líptiques sobre K_v amb bona reducció (a v). Però, ara, la cohomologia no-ramificada és isomorfa a $\mathbb{Z}/2\mathbb{Z}$. Per tant, per a cada $j \in K_v (j \neq 0, 1728)$ hom té cap, o bé dues corbes el·líptiques sobre K_v amb bona reducció i invariant modular j.

§1. El problema local.

Donada una valoració $v \in \Sigma$, es defineix $J(v)$ com el conjunt dels $j \in K$ tals que existeix una corba el·líptica E, definida sobre K, amb $j(E) = j$ i bona reducció a v.

REMARQUES 2.1:

1) $j \in J(v) \Longrightarrow j \in \mathcal{O}_v$.
2) Donada $j \in \mathcal{O}_v$, sigui E una corba el·líptica amb $j(E) = j$. Aleshores són equivalents:
   (i) $j \in J(v)$.
   (ii) Existeix un torcement de E amb bona reducció a v.
   (iii) Existeix $D \in K^*/K^{*^n}$, $n = 2, 4, 6$, tal que E^D té bona reducció a v.

Si Δ_E és el discriminant de E i $j \neq 0, 1728$, tindrem com a conseqüència:

$$v(\Delta_E) \equiv 0 \pmod 6$$

[vegi's Capítol 0].

Considerem, per $j \neq 0, 1728$, la corba el·líptica E_j, donada per la següent equació de Weierstraß afí:

$$y^2 = x^3 - \frac{27j}{j-1728}x - \frac{54j}{j-1728}. \tag{2.1}$$

Aleshores es té:

$$\Delta(E_j) = 6^{12} \cdot \frac{j^2}{(j-1728)^3}$$

$$\text{i } j(E_j) = j.$$

De les remarques 2.1, hom obté, així, una condició necessària per a $j \in J(v)$:

$$v(j) \geq 0, \qquad v(\Delta(E_j)) \equiv 0 \pmod 6$$

o, equivalentment:

$$v(j) \geq 0, \qquad v(j) \equiv 0 \pmod 3, \qquad v(j-1728) \equiv 0 \pmod 2. \tag{2.2}$$

Per a $p \neq 2, 3$, aquesta condició resulta ser suficient, cf. [Se-Ta], [Neum].

Tenim, doncs, una descripció senzilla de $J(v)$ per a $p \neq 2, 3$.

EXEMPLES 2.1:

1) Sigui E la corba el·líptica definida per la següent equació de Weierstraß afí:

$$E : y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728}.$$

Es té:

$$j(E) = j \text{ i } \Delta(E) = \frac{j^2}{(j-1728)^3}.$$

Per tant, donats $v \in \Sigma$, $j \in K$ amb $v(j) = v(j-1728) = 0$, E té bona reducció a v, és a dir, $j \in J(v)$.

De fet, la corba E_j resulta ser isomorfa a E^{-1}.

2) Per $p = 3$, $v \in \Sigma$, donem tres corbes el·líptiques amb invariant j satisfent (2.2), però, en canvi, $j \notin J(v)$:

   (a) $K = \mathbb{Q}(\sqrt[3]{3})$, $E : y^2 = x^3 - \frac{3\sqrt[3]{9}}{4}x - \frac{3}{2}$ amb $j(E) = -3^2 2^6$. Fent el canvi $u = \sqrt[3]{3}$, $r = \sqrt[3]{3}(\sqrt[3]{3}-1)$ tenim, per l'algoritme de Tate, que $\text{tip}(E) = \text{IV}$. Per tant, $j \notin J(v)$ (vegi's Cap. I, pàg. 15).

   (b) $K = \mathbb{Q}(\sqrt{3})$, $E : y^2 = x^3 + 9x + 3\sqrt{3}$ amb $j(E) = \frac{3^3 2^8}{5}$, $j - 1728 = -\frac{3^3 2^6}{5}$. Fent el canvi $r = -\sqrt{3}$, tenim que $\text{tip}(E) = \text{II}^*$. Per tant, $j \notin J(v)$.

   (c) $K = \mathbb{Q}(\sqrt{3})$, $E : y^2 = x^3 + \frac{9}{2}(1+\sqrt{3})x + (1+\sqrt{3})$ amb $j(E) = \frac{3^6 2^6(1+\sqrt{3})}{3^3(1+\sqrt{3})+2}$. Fent el canvi $r = -1$, tenim que $\text{tip}(E) = \text{II}$. Per tant, $j \notin J(v)$.

3) Per $p = 2$, $v \in \Sigma$, donem tres corbes el·líptiques amb invariant j satisfent (2.2), però, en canvi, $j \notin J(v)$:

   (a) $K = \mathbb{Q}(\sqrt[3]{2})$, $E : y^2 + 2xy + 2y = x^3 + \sqrt[3]{2}x$ amb $j(E) = \frac{2^8(5+3\sqrt[3]{2})^3}{(31+26\sqrt[3]{2}+23\sqrt[3]{4})}$. Per tant, $v(j) = 8e = 24$. Però, $\text{tip}(E) = \text{III}$ i per tant, $j \notin J(v)$ (vegi's cor. 1.1.1, 1.1.2. del Cap. I).

   (b) $K = \mathbb{Q}(\sqrt{2})$, $E : y^2 = x^3 - 3(21-17\sqrt{2})x - 4(55-38\sqrt{2})$ amb $j(E) = 2^6 3(13-4\sqrt{2})$ i $j - 1728 = 2^8 3(1-\sqrt{2})$. Fent el canvi $r = s = 1$, trobem que tip $E = \text{II}$ i pels cor. 1.1.1, 1.1.2 del Cap. I, $j \notin J(v)$.

   (c) $K = \mathbb{Q}(\sqrt[3]{2})$, $E : y^2 = x^3 - \frac{27(1+\sqrt[3]{2})}{\sqrt[3]{2}-107}x - \frac{54(1+\sqrt[3]{2})}{\sqrt[3]{2}-107}$ amb $j(E) = 2^4(1+\sqrt[3]{2})$.

   Fent el canvi $r = 3$, $s = 3$, $u = \sqrt[3]{2}$, obtenim un model de tipus II amb $v(b_2) = 4$ i $v(b_6) = 7$, per tant, pels T. 1.1, 1.2 del Cap. I, $j \notin J(v)$.

El nostre objectiu és donar una descripció explícita de $J(v)$ per a $p = 2, 3$. El cas no-ramificat ha sigut ja resolt per Neumann, [Neum], en els següents teoremes:

TEOREMA ([NEUM]).
$p = 2$, $v(2) = 1$, $j \in K$:

$$j \in J(v) \Longleftrightarrow \begin{cases} v(j) = v(j-1728) = 0 & \text{ó} \\ v(j) \geq 12,\ v(j) \equiv 0 \ (mod\ 3) \end{cases}$$

TEOREMA ([NEUM]).
$p = 3$, $v(3) = 1$, $j \in K$:

$$j \in J(v) \Longleftrightarrow \begin{cases} v(j) = v(j-1728) = 0 & \text{ó} \\ v(j-1728) \geq 6,\ v(j) = 3,\ v(j-1728) \equiv 0 \ (mod\ 2). \end{cases}$$

Definim per a j fixat, $j \neq 0, 1728$, els següents polinomis:

$$g(x) = 3x^4 - \frac{6 \cdot 27 \cdot j}{j-1728}x^2 - \frac{12 \cdot 54 \cdot j}{j-1728}x - \left(\frac{27j}{j-1728}\right)^2$$
$$f(x) = g'(x)/12 = x^3 - \frac{27j}{j-1728}x - \frac{54j}{j-1728}$$

$g(x)$, $f(x)$, són precisament els polinomis de les x-coordenades dels punts de 3-torsió, 2-torsió, respectivament, de la corba E_j; i posem:

$$\Delta = \Delta(E_j) = 6^{12} \cdot \frac{j^2}{(j-1728)^3}.$$

Utilitzarem el següent conveni: Direm que el polinomi $h(x) \in K[x]$ té una arrel (mod π^i), per a $i \in \mathbb{Z}$, si existeix $r \in K$ tal que $v(h(r)) \geq i$.

TEOREMA 2.1.
Sigui $p \neq 2$ i sigui $j \in \mathcal{O}_v$, $j \neq 0, 1728$. Aleshores $j \in J(v)$ si i sols si $v(\Delta) \equiv 0$ (mod 6) i $f(x)$ té una arrel mòdul $\pi^{v(\Delta)/2}$.

DEMOSTRACIÓ:
Considerem, per $j \neq 0, 1728$, la corba el·líptica E_j, donada per l'equació (2.1).
Per la remarca 2.1.2, es té que, per una valoració $v \in \Sigma$, $j \in J(v)$ si i sols si existeix $d \in K^*/K^{*2}$, tal que E_j^d té bona reducció a v.
En el cas $p \neq 2$, l'anterior condició és equivalent [vegi's Capítol I, pàg. 15] a cadascuna de les següents:

- E_j té bona reducció ó E_j^π té bona reducció a v.
- $\text{tip}(E_j) = \text{I}_0, \text{I}_0^*$ a v.

Tenim també, clarament:

$$v(\Delta(E_j)) = v(\Delta) \equiv 0 \pmod 6.$$

Suposem, doncs, $\text{tip}(E_j) = \text{I}_0$. Aleshores, fent un canvi de coordenades, podem aconseguir un model:

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6', \qquad a_i' \in \mathcal{O}_v \tag{2.3}$$

amb $v(\Delta') = 0$.

De les fórmules del canvi de coordenades entre (2.1) i (2.3) obtenim:

$$\begin{aligned} u^6 a_6' &= f(r) \\ u^{12}\Delta' &= \Delta \qquad r \in K, \qquad u \in K^* \end{aligned}$$

i d'aquí:

$$\begin{aligned} v(u) &= \frac{1}{12}v(\Delta) \\ v(f(r)) &\geq \frac{v(\Delta)}{2}. \end{aligned} \tag{2.4}$$

Si $\text{tip}(E_j) = \text{I}_0^*$, E_j^π tindrà bona reducció a v, i, per tant, podrem aconseguir un model (2.3) per a E_j^π. Novament, de les equacions del canvi obtenim:

$$\begin{aligned} u^6 a_6' &= \pi^3 f(r/\pi) \\ u^{12}\Delta' &= \pi^6 \Delta \qquad r \in K, \qquad u \in K^* \end{aligned}$$

i d'aquí:

$$\begin{aligned} v(u) &= \frac{v(\Delta)+6}{12} \\ v(f(r/\pi)) &\geq \frac{v(\Delta)}{2}. \end{aligned} \tag{2.5}$$

Això conclou la prova de la necessitat de les condicions del teorema.

Per a provar-ne la suficiència cal veure, en cada cas, que:

$$\begin{aligned} v(\Delta) \equiv 0 \pmod{12} &\Longrightarrow \text{tip}(E_j) = \text{I}_0 \\ v(\Delta) \equiv 6 \pmod 6 &\Longrightarrow \text{tip}(E_j) = \text{I}_0^*. \end{aligned}$$

Sigui r una arrel de $f(x)$ (mòd $\pi^{v(\Delta)/2}$). Veurem, en cada cas, que fent la traslació $x' = x + r$ obtenim un model (2.3) de E_j amb:

$$\begin{aligned} v(a_2') &\geq \frac{v(\Delta)}{6} \\ v(a_4') &\geq \frac{v(\Delta)}{3}. \end{aligned}$$

És clar que de $a'_6 = f(r)$ tenim:

$$v(a'_6) = v(f(r)) \geq \frac{v(\Delta)}{2}. \tag{2.6}$$

Si $v(\Delta) \equiv 0 \pmod{12}$, podrem dividir per $u = \pi^{\frac{v(\Delta)}{12}}$ i obtindrem un model per a E_j amb bona reducció a v.

Si $v(\Delta) \equiv 6 \pmod{12}$, dividint per $u = \pi^{\frac{v(\Delta)-6}{12}}$ obtindrem un model per a E_j de tipus I_0^* a v.

En efecte,

(i) $p = 3$, $0 \leq v(j) < 3e$.

Llavors, $v(\Delta) = 12e - v(j)$.

De (2.6) tenim que:

$$v(r) = \frac{1}{3} v\left(\frac{54j}{j - 1728}\right) = e$$

i, per tant, $v(a'_2) = v(3r) = 2e > \dfrac{v(\Delta)}{6}$.

Vegem, ara, que:

$$v(r + 3) \geq 2e - v(j)/3. \tag{2.7}$$

Efectivament, de (2.6) obtenim, multiplicant per $(j - 1728)$:

$$(j - 1728)r^3 - 27jr - 54j \equiv 0 \pmod{\pi^{\frac{v(\Delta)}{2} + v(j)}}$$

és a dir, $j(r + 3)^2(r - 6) - (12r)^3 \equiv 0 \pmod{\pi^{6e + v(j)/2}}$ i de $v(12r)^3 = 6e$ tenim:

$$2v(r + 3) + v(r - 6) = 6e - v(j). \tag{2.8}$$

Aleshores, $v(r + 3) < 2e - v(j)/3$ implicaria:

$$v(r - 6) = v(r + 3 - 9) = v(r + 3)$$
$$\text{i } 2v(r + 3) + v(r - 6) = 3v(r + 3) < 6e - v(j)$$

que contradiria (2.8).

Finalment, de

$$f(r) - \frac{rf'(r)}{3} = \frac{-18j}{j - 1728}(r + 3)$$

aplicant (2.7) tenim:

$$v(a'_4) = v(f'(r)) = v(f(r) - \frac{rf'(r)}{3}) \geq 2e + 2e - \frac{v(j)}{3} = \frac{v(\Delta)}{3}.$$

(ii) $p = 3$, $v(j) = 3e$, $v(j - 1728) < 6e$.
Llavors, $v(\Delta) = 18e - 3v(j - 1728)$.
De (2.6) tenim que:

$$v(r) = \frac{1}{3}v\left(\frac{54j}{j - 1728}\right) = 2e - v(j - 1728)/3$$

i, per tant,

$$v(a_2') = v(3r) = 3e - v(j - 1728)/3 > \frac{v(\Delta)}{6}.$$

Finalment, de

$$v(3r^2) = 5e - 2v(j - 1728)/3$$
$$v\left(\frac{-27j}{j - 1728}\right) = 6e - v(j - 1728)$$

es té:

$$v(a_4') \geq 6e - v(j - 1728) = \frac{v(\Delta)}{3}.$$

(iii) $p = 3$, $v(j) > 3e$.
Llavors, $v(\Delta) = 3e + 2v(j)$.
De (2.6) tenim que:

$$v(r) = \frac{1}{3}v\left(\frac{54j}{j - 1728}\right) = \frac{1}{3}v(j)$$

i, per tant,

$$v(a_2') = e + v(j)/3 > \frac{v(\Delta)}{6}.$$

Finalment, de $v(3r^2) = e + 2v(j)/3$, $v\left(\frac{27j}{j - 1728}\right) = v(j)$ es té:

$$v(a_4') \geq e + \frac{2}{3}v(j) = \frac{v(\Delta)}{3}.$$

(iv) $p = 3$, $v(j) = 3e$, $v(j - 1728) \geq 6e$.
Ara, $v(\Delta) = 18e - 3v(j - 1728) \leq 0$.
De (2.6) tenim que:

$$v(r) \geq 3e - \frac{1}{2}v(j - 1728)$$

i, per tant,

$$v(a_2') \geq 4e - \frac{1}{2}v(j - 1728) > \frac{v(\Delta)}{6}$$

i de

$$v(3r^2) \geq 7e - v(j-1728)$$
$$v\left(\frac{27j}{j-1728}\right) = 6e - v(j-1728)$$

es té:

$$v(a_4') \geq 6e - v(j-1728) = \frac{v(\Delta)}{3}.$$

(v) $p \neq 3$, $v(j) > 0$.
Llavors, $v(\Delta) = 2v(j)$.
De (2.6) tenim que:

$$v(r) \geq v(j)/3$$

i, per tant,

$$v(a_2') \geq v(j)/3 = \frac{v(\Delta)}{6}$$

i de

$$v(3r^2) \geq 2v(j)/3$$
$$v\left(\frac{27j}{j-1728}\right) = v(j)$$

es té:

$$v(a_4') \geq 2v(j)/3 = v(\Delta)/3.$$

(vi) $p \neq 3$, $v(j) = 0$.
Ara, $v(\Delta) = -3v(j-1728) \leq 0$.
De (2.6) tenim que:

$$v(r) \geq -v(j-1728)/2$$

i, per tant,

$$v(a_2') \geq -v(j-1728)/2 = \frac{v(\Delta)}{6}$$
$$v(a_4') \geq -v(j-1728) = \frac{v(\Delta)}{3}.$$

Aquest cas acaba la demostració del teorema ∎

COROL·LARI 2.1.1.
Sigui $p \neq 2$, 3 i sigui $j \in \mathcal{O}_v$, $j \neq 0$, 1728. Aleshores $j \in J(v)$ si i sols si $v(\Delta) \equiv 0$ (mod 6).

DEMOSTRACIÓ:

En efecte, en aquest cas, el polinomi $f(x)$ té sempre una arrel, r, mòdul $\pi^{v(\Delta)/2}$. Per exemple, $r = 0$ ∎

COROL·LARI 2.1.2.

Sigui $p = 3$ i $j \in \mathcal{O}_v$, $j \neq 0, 1728$. Aleshores $j \in J(v)$ si i sols si $v(\Delta) \equiv 0$ (mod 6) i $f(x)$ té una arrel mòdul $\pi^{v(\Delta)/2}$ quan $v(\Delta) > 0$.

DEMOSTRACIÓ:

En efecte, $f(x)$ té sempre una arrel, r, mòdul $\pi^{v(\Delta)/2}$ quan $v(\Delta) \leq 0$. Per exemple, $r = 0$ ∎

COROL·LARI 2.1.3.

Sigui $p = 3$ i sigui $j \in \mathcal{O}_v$, $j \neq 0, 1728$. Aleshores $j \in J(v)$ si i sols si es satisfà alguna de les condicions següents:

(i) $v(j) = v(j - 1728) = 0$.
(ii) $v(j) = 3e$, $v(j - 1728) \geq 6e$, $v(j - 1728) \equiv 0$ (mod 2).
(iii) $v(j) = 3e$, $v(j - 1728) < 6e$, $v(j - 1728) \equiv 0$ (mod 6) i $f(x)$ té una arrel (mod $\pi^{9e - \frac{3}{2}v(j-1728)}$).
(iv) $v(j) < 3e$, $v(j) \equiv 0$ (mod 6) i $f(x)$ té una arrel (mod $\pi^{6e - v(j)/2}$).
(v) $v(j) > 3e$, $v(j) \equiv 0$ (mod 3), $e \equiv 0$ (mod 2) i $f(x)$ té una arrel (mod $\pi^{3\frac{e}{2} + v(j)}$).

DEMOSTRACIÓ:

En efecte, pel cas (i) vegi's l'exemple 2.1.1. Les condicions (ii) a (v) s'obtenen en explicitar $v(\Delta)$ i la relació $v(\Delta) \equiv 0$ (mod 6) en cada cas. En la condició (iii), però, hom obté $v(j - 1728) \equiv 0$ (mod 6) de $v(j - 1728) \equiv 0$ (mod 2) i del fet que la valoració de l'arrel de $f(x)$ ha d'ésser $2e - v(j - 1728)/3$ ∎

REMARQUES 2.2:

1) La condició que, en l'enunciat del teorema 2.1, ha de satisfer el polinomi $f(x)$ és equivalent a l'existència d'un punt de 2-torsió racional mòdul $\pi^{v(\Delta)/2}$ per a la corba el·líptica E_j.
2) Per $j \in J(v)$, $p \neq 2$. Posem:

$$D = \begin{cases} \pi & \text{si } v(\Delta) \equiv 6 \pmod{12} \\ 1 & \text{si } v(\Delta) \equiv 0 \pmod{12}. \end{cases}$$

En la demostració del teorema 2.1 hem provat que:

$$E_j^D \text{ té bona reducció a } v.$$

3) Del corol·lari 2.1.3, per $v(3) = 1$, s'obté de manera directa el Teorema de Neumann per $p = 3$.
4) Per $p = 2$, $v \in \Sigma$, l'invariant j de l'exemple 2.1.3 (b) satisfà les hipòtesis del Teorema 2.1. Però, en canvi, $j \notin J(v)$.

TEOREMA 2.2.

Sigui $p = 2$ i sigui $j \in \mathcal{O}_v$, $j \neq 0, 1728$. Aleshores $j \in J(v)$ si i sols si $v(\Delta) \equiv 0$ (mod 6) i $g(x)$ té una arrel mòdul $\pi^{2v(\Delta)/3}$.

Abans de demostrar el teorema, enunciem i provem el següent lema:

LEMA 2.

Siguin $p = 2$, $v(j) \geq 0$, $v(\Delta) \equiv 0$ (mod 6). Si $g(x)$ té una arrel, r, mòdul $\pi^{2v(\Delta)/3}$ aleshores, necessàriament, $v(g'(r)) = v(\Delta)/2$.

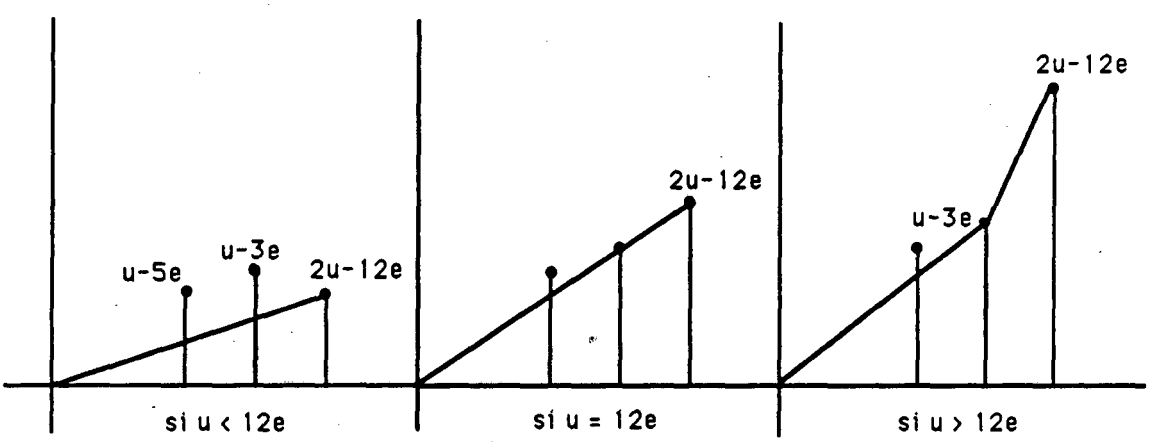
DEMOSTRACIÓ:

Posem $b = j/j - 1728$, $u = v(j)$, i considerem els polinomis:

$$g(x) := 3^{-5}g(3x) = x^4 - 6bx^2 - 8bx - 3b^2$$
$$g'(x) := 3^{-4}g'(3x) = 4(x^3 - 3bx - 2b).$$

(i) $u > 6e$.

En aquest cas, $v(b) = u - 6e$, $v(\Delta) = 2u - 6e$. El polígon de Newton de $g(x)$ és:



Per tant, en els dos primers casos la condició:

$$v(g(x)) \geq 2v(\Delta)/3, \qquad x \in \mathcal{O}_v$$

implica $v(x) = \frac{u}{2} - 3e$, mentre que en el darrer cas es té: $v(x) \geq \frac{u}{3} - e$.

Si $u > 8e$, es té en qualsevol cas:

$$v(x^3 - 3bx) > u - 5e \tag{2.9}$$

i d'aquí: $v(g'(x)) = 2e + v(2b) = u - 3e$.

Suposem $u \leq 8e$. Llavors:

$$v(x^3 - 3bx) = \frac{u}{2} - 3e + v(x^2 - 3b).$$

Però de:

$$g(x) = (x^2 - 3b)^2 - 12b^2 - 8bx$$

tenim $v(x^2 - 3b) > \frac{u}{2} - 2e$.

Per tant, novament es verifica (2.9) i, d'aquí, el resultat volgut.

(ii) $u < 6e$.

En aquest cas tenim:

$$v(b-1) = 6e - u, \qquad v(\Delta) = 12e - u.$$

Desenvolupant $g(x)$ respecte de la variable $x+1$ tenim:

(2.10)

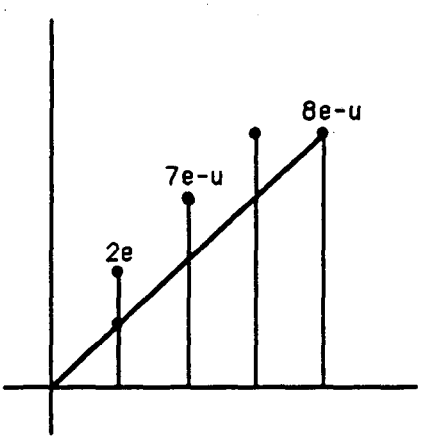
$$g(x) = (x+1)^4 - 4(x+1)^3 - 6(b-1)(x+1)^2 + 4(b-1)(x+1) - (b-1)(3b+1)$$

$$g'(x) = 4[(x+1)^3 - 3(x+1)^2 - 3(b-1)(x+1) + b - 1].$$

Es té la relació:

$$g(x) = xg'(x) - 3[b - 1 + 2(x+1) - (x+1)^2]^2. \tag{2.11}$$

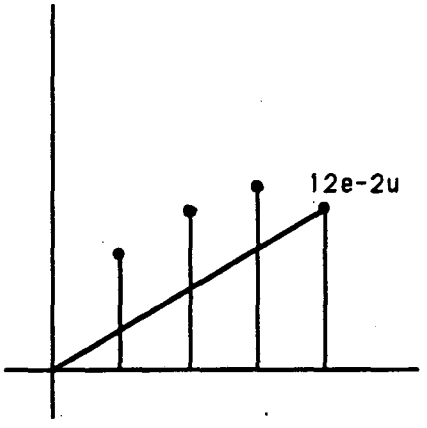
Suposem, primer, $u < 4e$. Aleshores, $v(3b+1) = 2e$ i pel polígon de Newton de $g(x)$ es té:



$$v(x+1) = 2e - \frac{u}{4}$$

Per tant, $v(b - 1 + 2(x+1) - (x+1)^2) = 3e - \frac{u}{4}$ i de (2.11) s'obté la valoració volguda per a $g'(x)$.

Suposem, ara, $4e < u < 6e$. Aleshores, $v(3b+1) = 6e - u$ i pel polígon de Newton de $g(x)$ es té:



$$v(x+1) = 3e - \frac{u}{2}$$

De (2.10): $v(g'(x)) \geq 8e - u$
i de (2.11): $v(b-1-(x+1)^2) = 4e - \frac{u}{2}$.
D'aquí:

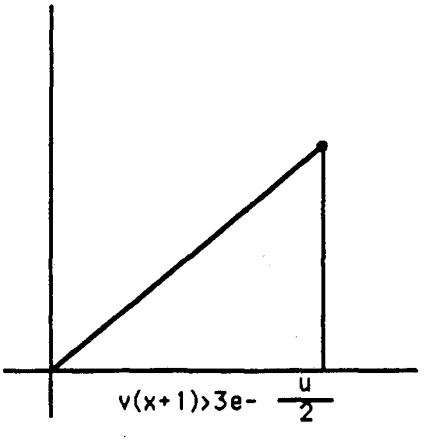
$$v(-3(x+1)^2 + b - 1) = 4e - \frac{u}{2}$$
$$v((x+1)^2 - 3(b-1)) = 4e - \frac{u}{2}$$

i de (2.10) s'obté directament el resultat desitjat.

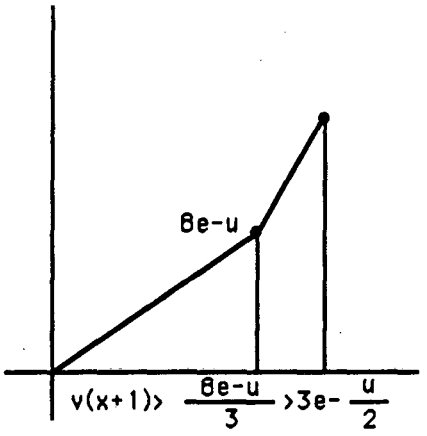
Suposem, finalment, $u = 4e$.

Si $v(3b+1) = 6e - u$, s'aplica el mateix raonament del cas anterior.

Si $v(3b+1) > 6e - u$, el polígon de Newton de $g(x)$ serà:



o bé,



Per tant, en qualsevol cas tindrem:

$$v(x+1) > 3e - \frac{u}{2} = e$$

i, de (2.10) obtenim: $v(g'(x)) = 4e$.

(iii) $u = 6e$.

Posem, ara, $c = j - 1728$, $w = v(c)$ i considerem els polinomis:

$$\tilde{g}(x) = c^4 g(x/c) = x^4 - 6jcx^2 - 8jc^2x - 3j^2c^2$$
$$\tilde{g}'(x) = 4(x^3 - 3jcx - 2jc^2).$$

Per hipòtesi, doncs:

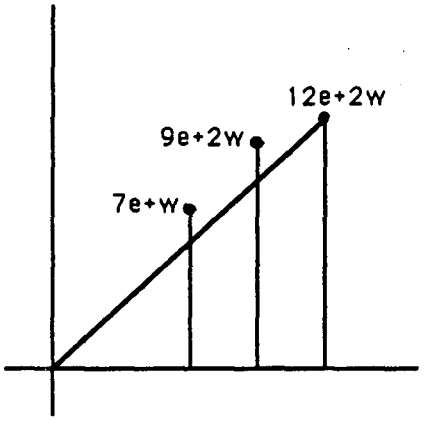
$$v(\tilde{g}(x)) \geq \frac{2v(\Delta)}{3} + 4w, \qquad x \in \mathcal{O}_v$$

on $v(\Delta) = 24e - 3w$.

Es tracta de provar:

$$v(\tilde{g}'(x)) = \frac{v(\Delta)}{2} + 3w = 12e + \frac{3}{2}w. \tag{2.12}$$

Considerem el polígon de Newton de $\tilde{g}(x)$:



Aleshores tenim, $v(x) = 3e + \frac{w}{2}$.

Posem

$$\tilde{g}(x) = (x^2 - 3jc)^2 - 12j^2c^2 - 8jc^2x$$
$$\tilde{g}'(x) = 4[x(x^2 - 3jc) - 2jc^2].$$

De la primera igualtat obtenim:

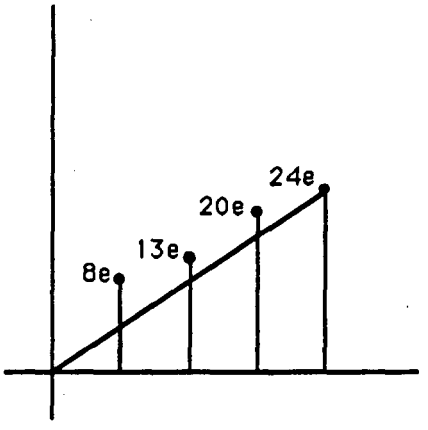
$$v(x^2 - 3jc) = 7e + w$$

i, si $w > 6e$, de la segona igualtat n'obtenim directament (2.12).

Si $w = 6e$, considerem el desenvolupament de $\tilde{g}(x)$ respecte de $(x + j)$:

$$\tilde{g}(x) = (x+j)^4 - 4j(x+j)^3 - 6j(c-j)(x+j)^2 - 4(j^3 - 2jc^2 + 3j^2c)(x+j) + \tilde{g}(-j).$$

Dibuixant el polígon de Newton:



tenim: $v(x + j) = 6e$.

De la relació:

$$\tilde{g}(x) = x \cdot \tilde{g}'(x) - 3[x^2 - cj]^2$$

tenim que:

$$v(x^2 - jc) > 13e$$

ja que $v(\tilde{g}'(x)) \geq 21e$.

Finalment, de la igualtat:

$$\tilde{g}(x) = \frac{x \cdot \tilde{g}'(x)}{4} - 3jc[x^2 - jc + 2c(x + j)]$$

obtenim $v(\tilde{g}'(x)) = 21e$ ∎

DEMOSTRACIÓ DEL TEOREMA 2.2:

Sigui $d \in K^*/K^{*^2}$ tal que E_j^d té bona reducció a v. Considerem el model per E_j^d següent:

$$y^2 = x^3 - \frac{27j}{j-1728}d^2x - \frac{54j}{j-1728}d^3 \tag{2.13}$$

amb $\Delta(E_j^d) = d^6\Delta$.

Pel fet de tenir E_j^d bona reducció a v, existirà un model

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \tag{2.14}$$

amb $v(\Delta') = 0$.

Per les fórmules del canvi de variables entre (2.13) i (2.14) (Cap. 0) tindrem:

$$\begin{aligned} &u^{12}\Delta' = d^6\Delta \\ &u^8 b_8' = d^4 g(r/d) \qquad r \in K, \qquad u \in K^* \end{aligned}$$

i d'aquí:

$$\begin{aligned} v(u) &= \frac{6v(d) + v(\Delta)}{12} \\ v(g(r/d)) &\geq 2v(\Delta)/3. \end{aligned} \tag{2.15}$$

Això conclou la prova de la necessitat de les condicions del teorema.

Per a provar-ne la suficiència, considerem r arrel de $g(x)$ mòdul $\pi^{2v(\Delta)/3}$. Aleshores afirmem que la corba el·líptica $E_j^{f(r)}$, obtinguda torçant E_j per $d = f(r)$, té bona reducció a v.

En efecte, considerem el model (2.13) per $E_j^{f(r)}$ i apliquem-li el canvi de coordenades:

$$\begin{aligned} x &= u^2x' + R \\ y &= u^3y' + u^2Sx' + T \end{aligned}$$

essent:

$$u = \frac{1}{2}, \qquad R = rf(r), \qquad S = \frac{1}{2}f'(r), \qquad T = f^2(r).$$

Obtenim així una corba el·líptica isomorfa, amb model (2.14), on:

$$\begin{aligned} a_1' &= 2f'(r) & a_2' &= g(r) \\ a_3' &= 2^4 f^2(r) & a_4' &= a_6' = 0 \end{aligned}$$

i $\Delta' = 2^{12} f^6(r)\Delta$.

De les hipòtesis i el lema 2, tenim:

$$v(f(r)) = v\left(\frac{1}{4}g'(r)\right) = \frac{v(\Delta)}{2} - 2e.$$

Per tant,

$$v(\Delta') = 12e + 6\left(\frac{v(\Delta)}{2} - 2e\right) + v(\Delta) = 4v(\Delta)$$
$$v(a_2') = v(g(r)) \geq \frac{2}{3}v(\Delta)$$
$$v(a_3') = 4e + 2\left(\frac{v(\Delta)}{2} - 2e\right) = v(\Delta).$$

Finalment, per a poder dividir per $\pi^{v(\Delta)/3}$, ens cal veure que:

$$v(a_1') = v(2f'(r)) \geq \frac{v(\Delta)}{3}. \tag{2.16}$$

En efecte, calculant el polígon de Newton de $g(x)$, sempre es satisfà:

$$v(r) \geq \frac{v(\Delta)}{6} - 2e$$

(vegi's demostració del lema 2).

A partir de l'anterior desigualtat, i utilitzant la relació:

$$g(r) = 3rg'(r) - (f'(r))^2$$

s'obté directament (2.16). Això acaba la demostració ∎

COROL·LARI 2.2.1.

Sigui $p = 2$, i sigui $j \in \mathcal{O}_v$, $j \neq 0, 1728$. Aleshores $j \in J(v)$ si i sols si es satisfà una de les següents condicions:

(i) $v(j) < 12e$, $v(j) \equiv 0$ *(mod 12) i el polinomi $g(x)$ té una arrel mòdul $\pi^{\frac{2}{3}v(\Delta)}$. A més, $v(j - 1728) \equiv 0$ (mod 2) si $v(j) = 6e$.*

(ii) $v(j) \geq 12e$, $v(j) \equiv 0$ *(mod 3).*

DEMOSTRACIÓ:

En efecte, la relació $v(\Delta) \equiv 0 \pmod 6$ és equivalent a:

(i) $v(j) < 6e$, $v(j) \equiv 0 \pmod 6$.
(ii) $v(j) = 6e$, $v(j - 1728) \equiv 0 \pmod 2$.
(iii) $v(j) > 6e$, $v(j) \equiv 0 \pmod 3$.

De la igualtat:

$$g(x) = 3xg'(x) - [f'(x)]^2$$

obtenim:

$$v(x) + \frac{v(\Delta)}{2} \equiv 0 \pmod 2$$

on

$$v(x) = \begin{cases} 3e - v(j-1728)/2 & \text{si } v(j) = 6e \\ 0 & \text{si } v(j) < 6e \\ v(j)/2 - 3e & \text{si } 6e < v(j) < 12e \end{cases}$$

d'aquí, doncs, tenim:

$$e \equiv 0 \pmod 2 \text{ si } v(j) = 6e$$
$$v(j) \equiv 0 \pmod 4 \text{ si } 0 \leq v(j) < 12e,\ v(j) \neq 6e.$$

Finalment, quan $v(j) \geq 12e$, $g(x)$ té sempre una arrel, r, mòdul $\pi^{\frac{2}{3}v(\Delta)}$. Per exemple, $r = 0$ ∎

COROL·LARI 2.2.2.

Sigui $p = 2$ i sigui $j \in \mathcal{O}_v$, $j \neq 0, 1728$. Aleshores $j \in J(v)$ si i sols si es satisfà alguna de les següents condicions:

(i) $v(j) = v(j-1728) = 0$.
(ii) $v(j) < 6e$, $v(j) \equiv 0$ *(mod 12) i* $g(x)$ *té una arrel (mod* $\pi^{8e-\frac{2}{3}v(j)}$*).*
(iii) $v(j) = 6e$, $v(j-1728) \equiv e \equiv 0$ *(mod 2) i* $g(x)$ *té una arrel (mod* $\pi^{16e-2v(j-1728)}$*).*
(iv) $6e < v(j) < 12e$, $v(j) \equiv 0$ *(mod 12) i* $g(x)$ *té una arrel (mod* $\pi^{\frac{4}{3}v(j)-4e}$*).*
(v) $v(j) \geq 12e$ *i* $v(j) \equiv 0$ *(mod 3).*

DEMOSTRACIÓ:

En efecte, pel cas (i) vegi's exemple 2.1.1. Les condicions (ii) a (v) s'obtenen del corol·lari 2.2.1, en explicitar $v(\Delta)$ en cada cas ∎

REMARQUES 2.3:

1) La condició que, en l'enunciat del teorema 2.2, ha de satisfer el polinomi $g(x)$ és equivalent a l'existència d'una x-coordenada de 3-torsió racional mòdul $\pi^{2v(\Delta)/3}$ per a E_j.
2) Per $p = 2$, $j \in J(v)$, sigui $r \in K$ una arrel de $g(x)$ mòdul $\pi^{2v(\Delta)/3}$. Posem $D = f(r)$. En la demostració del teorema 2.2 hem provat que:

$$E_j^D \text{ té bona reducció a } v.$$

De fet, l'exemple 2.1.1 i la demostració del corol·lari 2.2.1 ens mostren que podem prendre:

$$D = \begin{cases} -1, & \text{si } v(j) = 0 \\ \dfrac{-6j}{j-1728}, & \text{si } v(j) \geq 12e. \end{cases}$$

3) Del corol·lari 2.2.2, per $v(2) = 1$, s'obté directament el Teorema de Neumann per $p = 2$.
4) Per $p = 3$, $v \in \Sigma$, l'invariant j de l'exemple 2.1.2 (c) satisfà les hipòtesis del Teorema 2.2, però, $j \notin J(v)$.

Fins aquí, hem donat unes condicions necessàries i suficients per a, donat un $j \in K$ i una valoració $v \in \Sigma$, tenir $j \in J(v)$, però amb $j \neq 0, 1728$.

Neumann, en el seu treball [Neum], ja va resoldre el problema per a $j = 0, 1728$. Anem a enunciar aquests resultats, en les proposicions que segueixen, donant una demostració nostra de les mateixes, la qual ens serà útil més endavant (vegi's remarques 2.4).

PROPOSICIÓ 2.1.

Per $j = 0, v \in \Sigma$ es té $j \in J(v)$ si i sols si $p \neq 3$ o $p = 3$ i $K(\sqrt{-3})|K$ és no-ramificada a v.

DEMOSTRACIÓ:

Considerem la corba el·líptica E_j, amb el següent model de Weiestraß:

$$E_j : y^2 + y = x^3.$$

Tenim $\Delta(E_j) = -27$, $j(E_j) = 0$. Per tant, E_j té bona reducció a tot $v \in \Sigma$, $v \nmid 3$.

Sigui, ara, $v \in \Sigma$, $v|3$ i suposem $0 \in J(v)$. Denotem per E_j^d, $d \in K^*/K^{*6}$, la corba el·líptica E_j torçada per d, amb model de Weierstraß:

$$y^2 = x^3 + 2^4 d.$$

E_j^d té, per hipòtesi, bona reducció a v, per a un cert d. Aleshores, de

$$\Delta(E_j^d) = -27 \cdot 2^{12} \cdot d^2$$
$$\text{i } v(\Delta(E_j^d)) \equiv 0 \pmod{12}$$

tenim: $3e + 2v(d) \equiv 0 \pmod{12}$ i d'aquí: $e \equiv 0 \pmod 2$.

Per a provar la suficiència, posem, per $v \in \Sigma$, $v|3$:

$$d = 4\pi^{3e/2}.$$

Vegem que E_j^d té bona reducció a v. En efecte, fent el canvi:

$$x = x' + r$$
$$y = y'$$

amb $r = -4\pi^{e/2}$, obtenim un model (2.14) E' amb:

$$a'_1 = a'_3 = a'_6 = 0 \qquad a'_4 = 32^4\pi^e$$
$$a'_2 = -12\pi^{e/2} \qquad \Delta(E') = -27\pi^{3e}2^{18}.$$

Per tant, $v(\Delta(E')) = 6e$, $v(a'_2) = 3e/2$, $v(a'_4) = 2e$ i podem dividir per $\pi^{e/2}$ ∎

PROPOSICIÓ 2.2.

Per $j = 1728$, $v \in \Sigma$ es té $j \in J(v)$ si i sols si $p \neq 2$ o $p = 2$ i $K(\sqrt{-1})|K$ és no-ramificada a v.

DEMOSTRACIÓ:

Considerem la corba el·líptica E_j, amb el següent model de Weierstraß:

$$E_j : y^2 = x^3 + x.$$

Llavors, $\Delta(E_j) = -64$, $j(E_j) = 1728$.

Per tant, E_j té bona reducció a $v \in \Sigma$, per a tot $v \not| 2$.

Sigui, ara, $v \in \Sigma$, $v|2$ i suposem $1728 \in J(v)$. Denotem per E_j^d, $d \in K^*/K^{*4}$, la corba el·líptica torçada per d, amb model de Weierstraß:

$$y^2 = x^3 + dx$$

i $\Delta(E_j^d) = -64d^3$.

Existeix, doncs, per hipòtesis, un d tal que E_j^d té bona reducció a v. Per tant, podrem trobar un model (2.14) E', amb $v(\Delta(E')) = 0$. De les equacions del canvi de variables obtenim:

$$u^{12}\Delta(E') = -64d^3$$
$$u^8 b'_8 = -d^2 + 6r^2d + 3r^4, \qquad r \in K, \qquad u \in K^*$$

i d'aquí:

$$v(u) = \frac{e}{2} + \frac{1}{4}v(d)$$

$$-d^2 + 6r^2d + 3r^4 = 3(r^2 + d)^2 - 4d^2 \equiv 0 \pmod{\pi^{4e+2v(d)}}$$

per tant,

$$-1 \equiv 3 \equiv \left(\frac{2d}{r^2 + d}\right)^2 \pmod{\pi^{2e}}.$$

Això prova la necessitat de la condició de la proposició. Per a veure'n la suficiència, sigui $\alpha \in K^*$ tal que:

$$-1 \equiv \alpha^2 (\text{mod } \pi^{2e}), \qquad v \in \Sigma, \qquad v|2$$

i posem $d = (\alpha+1)^2 - 1$.

Vegem que E_j^d té bona reducció a v. En efecte, fent el canvi:

$$x = x' + r$$
$$y = y' + sx' + t$$

amb $r = \dfrac{1}{\alpha^2}$, $s = 1$, $t = -\dfrac{1+\alpha}{\alpha^3}$, obtenim un model (2.14) E' amb $v(\Delta(E')) = 6e$ i

$$a'_1 = 2 \qquad a'_4 = \frac{1}{\alpha^4}(\alpha^6 + 2\alpha^5 + 2\alpha^2 + 2\alpha + 3)$$
$$a'_2 = \frac{3-\alpha^2}{\alpha^2} \qquad a'_6 = \frac{1}{\alpha^5}(\alpha^5 + 2\alpha^4 - \alpha - 2)$$
$$a'_3 = -2(1+\alpha)/\alpha^3$$

Per tant, $v(a'_1) = e$, $v(a'_2) \geq 2e$, $v(a'_3) = 3e/2$ i de $\alpha^4 \equiv 1 \ (\text{mod } \pi^{3e})$ tenim:

$$\alpha^6 + 2\alpha^5 + 2\alpha^2 + 2\alpha + 3 \equiv 3(\alpha^2+1) + 4\alpha \ (\text{mod } \pi^{3e})$$
$$\alpha^5 + 2\alpha^4 - \alpha - 2 \equiv 0 \ (\text{mod } \pi^{3e})$$

d'aquí:

$$v(a'_4) \geq 2e$$
$$v(a'_6) \geq 3e.$$

Per tant, podem dividir per $\pi^{\frac{6}{2}}$ i això acaba la demostració ∎

REMARQUES 2.4:

1) Per $j = 0$, $v \in \Sigma$, $j \in J(v)$ si $p = 3$, sigui E_j la corba el·líptica: $y^2 + y = x^3$.
   Posem:
$$D = \begin{cases} 1 & \text{si } p \neq 3 \\ 4\pi^{3e/2} & \text{si } p = 3. \end{cases}$$
   Aleshores, en la demostració de la proposició 2.1 hem provat que E_j^D té bona reducció a v.

2) Per $j = 1728$, $v \in \Sigma$, $j \in J(v)$ si $p = 2$, sigui E_j la corba el·líptica: $y^2 = x^3 + x$.
   Posem:
$$D = \begin{cases} 1 & \text{si } p \neq 2 \\ (\alpha+1)^2 - 1 & \text{si } p = 2 \end{cases}$$
   on $\alpha^2 + 1 \equiv 0 \ (\text{mod } \pi^{2e})$.
   Aleshores, en la demostració de la proposició 2.2 hem provat que E_j^D té bona reducció a v.

§2. El problema global.

Donat S, subconjunt finit de Σ, definim els conjunts $J(\Sigma\backslash S)$, J_S així:

$J(\Sigma\backslash S) = \{j \in K : j \in J(v)$ per a tot $v \in \Sigma\backslash S\}$

$J_S = \{j \in K :$ existeix una corba el·líptica E, definida a K, amb $j(E) = j$ i bona reducció arreu, fora de $S\}$.

REMARQUES 2.5:

1) $J(\Sigma\backslash S) \supseteq J_S$.
2) $j \in J(\Sigma\backslash S) \Longrightarrow v(j) \geq 0$ per a tot $v \in \Sigma\backslash S$.
3) Donada $j \in J(\Sigma\backslash S)$, sigui E una corba el·líptica amb $j(E) = j$ i sigui $(d_v)_{v\in\Sigma\backslash S} \in \prod_{v\in\Sigma\backslash S} K_v^*/K_v^{*n}$ tal que E^{d_v} té bona reducció a v, per a cada $v \in \Sigma\backslash S$. Aleshores, són equivalents:
   (i) $j \in J_S$.
   (ii) Existeix un torcement de E amb bona reducció arreu, fora de S.
   (iii) Existeix $D \in H^1(G_K, \mu_n)$ tal que E^D té bona reducció arreu, fora de S.
   (iv) Existeix $D \in H^1(G_K, \mu_n)$ tal que:

$$d_v/D \in H^1_{nr}(G_v, \mu_n) \text{ per a tot } v \in \Sigma\backslash S.$$

El nostre objectiu és donar una descripció explícita de J_S, vist com a subconjunt de $J(\Sigma\backslash S)$.

Per això, notarem per:

$$\mathcal{U}_S(n) := \{a \in K^* | a \in \mathcal{U}_v \text{ per } v \in \Sigma\backslash S,\ a \in K_v^{*n} \text{ per } v \in S \cup \Sigma^\infty\}$$

$_n(\ ,\ )_v$: el símbol de Hilbert local en v, relatiu a μ_n i calculat, per tant, a $K_v(\mu_n)$ on

$$n = \begin{cases} 2 & \text{si } j \neq 0, 1728 \\ 4 & \text{si } j = 1728 \\ 6 & \text{si } j = 0. \end{cases}$$

TEOREMA 2.3.

Per a $j \in J(\Sigma\backslash S)$, sigui $(d_v)_{v\in\Sigma\backslash S} \in \prod_{v\in\Sigma\backslash S} K_v^*/K_v^{*n}$ tal que $E_j^{d_v}$ té bona reducció a v, per a cada $v \in \Sigma\backslash S$. Aleshores, $j \in J_S$ si i sols si:

$$\prod_{v\in\Sigma\backslash S} {}_n(d_v, u)_v = 1 \qquad \forall u \in \mathcal{U}_S(n)/(K^{*n} \cap \mathcal{U}_S(n)).$$

DEMOSTRACIÓ:

Per $v \in \bar{\Sigma} := \Sigma \cup \Sigma^{\infty}$, siguin:

$$G_K = \mathrm{Gal}(\bar{K}|K)\ ,\ G'_K = \mathrm{Gal}(\bar{K}|K(\mu_n))$$
$$G_v = \mathrm{Gal}(\bar{K}_v|K_v)\ ,\ G'_v = \mathrm{Gal}(\bar{K}_v|K_v(\mu_n)).$$

Sigui $H^1_{nr}(G_v, \mu_n)$ el subgrup de $H^1(G_v, \mu_n)$ dels torcements locals no-ramificats, i considerem: $\prod_{v\in\bar{\Sigma}} H^1(G_v, \mu_n)$, el producte restringit de $H^1(G_v, \mu_n)$ respecte de $H^1_{nr}(G_v, \mu_n)$.

Considerem, també, el morfisme canònic de restricció:

$$\rho : H^1(G_K, \mu_n) \longrightarrow \prod_{v\in\bar{\Sigma}} H^1(G_v, \mu_n).$$

Donat $j \in J(\Sigma\backslash S)$, $v \in \bar{\Sigma}$, sigui:

$$D_v = \begin{cases} d_v & \text{si } v \in \Sigma\backslash S \\ 1 & \text{si } v \in \Sigma^{\infty} \cup S. \end{cases}$$

Tenim, doncs, $(D_v)_v \in \prod_{v\in\bar{\Sigma}} H^1(G_v, \mu_n)$.

Definim, ara:

$$V := \prod_{v\in S\cup\Sigma^{\infty}} H^1(G_v, \mu_n) \times \prod_{v\in\Sigma\backslash S} H^1_{nr}(G_v, \mu_n) \leq \prod_{v\in\bar{\Sigma}} H^1(G_v, \mu_n).$$

Aleshores, per la remarca 2.5.3, són equivalents:

- $j \in J_S$
- $(D_v)_v \in (\mathrm{Im}\rho) \cdot V$.

Per la dualitat de Tate-Poitou (cf. [Neuk]) tenim que l'aparellament:

$$\langle , \rangle : \prod_{v\in\bar{\Sigma}} H^1(G_v, \mu_n) \times \prod_{v\in\bar{\Sigma}} H^1(G_v, \mu_n) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

definit per:

$$\langle (a_v)_v, (b_v)_v \rangle = \prod_{v\in\bar{\Sigma}} {}_n(a_v, b_v)_v$$

és una dualitat perfecta i $\mathrm{Im}\rho$ és autoortogonal per aquesta dualitat.

Aleshores:

$$(\mathrm{Im}\rho \cdot V)^{\perp} = (\mathrm{Im}\rho)^{\perp} \cap V^{\perp} = \mathrm{Im}\rho \cap V^{\perp}.$$

Anem, ara, a veure que:

$$V^{\perp} = \prod_{v\in\Sigma\setminus S} \mathcal{U}_v/\mathcal{U}_v^n \times \prod_{v\in S\cup\Sigma^{\infty}} \{1\}. \tag{2.17}$$

En efecte, si $(x_v)_v \in V$ es té:

$$_n(x_v, 1)_v = 1, \text{ si } v \in S \cup \Sigma^{\infty}.$$

Mentre que, si $v \in \Sigma\setminus S$ llavors $x_v \in H^1_{nr}(G_v, \mu_n)$. Però, per ésser $K(\mu_n)|K$ no-ramificada a v (vegi's proposicions 2.1 i 2.2) tenim:

$$x_v \in H^1_{nr}(G_v, \mu_n) \Longleftrightarrow x_v \in H^1_{nr}(G'_v, \mu_n).$$

Per tant, $_n(x_v, y_v)_v = {}_n(x_v, y_v)_v^{-1} = 1$, $y_v \in \mathcal{U}_v/\mathcal{U}_v^n$.

Recíprocament, donat $(x_v)_v \in \prod_{v\in\bar{\Sigma}} H^1(G_v, \mu_n)$ i tal que:

$$\langle (x_v)_v, (y_v)_v \rangle = 1 \qquad \forall (y_v)_v \in \prod_{v\in\Sigma\setminus S} \mathcal{U}_v/\mathcal{U}_v^n \times \prod_{v\in S\cup\Sigma^{\infty}} \{1\}$$

definim, per $v_0 \in \Sigma\setminus S$:

$$(y_v)_v = \begin{cases} y_{v_0} \in \mathcal{U}_v/\mathcal{U}_v^n & \text{si } v = v_0 \\ 1 & \text{si } v \neq v_0. \end{cases}$$

Llavors:

$$1 = \langle (x_v)_v, (y_v)_v \rangle = {}_n(x_{v_0}, y_{v_0})_{v_0}$$

Però de $\mathcal{U}_v/\mathcal{U}_v^n = \left(H^1_{nr}(G'_v, \mu_n)\right)^{\perp}$ tenim que $(\mathcal{U}_v/\mathcal{U}_v^n)^{\perp} = H^1_{nr}(G'v, \mu_n)$ i, per tant, $x_{v_0} \in H^1_{nr}(G_{v_0}, \mu_n)$.

Amb això queda provat (2.17) i d'aquí obtenim:

$$(Im\rho \cdot V)^{\perp} = Im\rho \cap \left(\prod_{v\in\Sigma\setminus S} \mathcal{U}_v/\mathcal{U}_v^n \times \prod_{v\in S\cup\Sigma^{\infty}} \{1\} \right) = \mathcal{U}_S(n)/(K^{*^n} \cap \mathcal{U}_S(n)).$$

Finalment,

$$\begin{aligned} (D_v)_v \in (Im\rho)\cdot V &\Longleftrightarrow \langle (D_v)_v, u \rangle = 1 \qquad \forall u \in \mathcal{U}_S(n)/(K^{*^n} \cap \mathcal{U}_S(n)) \\ &\Longleftrightarrow \prod_{v\in\Sigma\setminus S} {}_n(D_v, u)_v = 1 \quad \forall u \in \mathcal{U}_S(n)/(K^{*^n} \cap \mathcal{U}_S(n)) \blacksquare \end{aligned}$$

REMARCA 2.6:
Del Teorema 2.3 es desprèn que, quan $K = \mathbb{Q}$:

$$j \in J_S \Longleftrightarrow j \in J(\Sigma \backslash S).$$

És a dir, en el cas particular dels nombres racionals no hi ha obstrucció local-global.

Per a estudiar l'existència de corbes el·líptiques amb conductor trivial i invariant j fixat, considerem $S = \phi$ i posem:

$$J(\Sigma) := J(\Sigma \backslash S)$$
$$J := J_S.$$

Observem que, en aquest cas:

$$\mathcal{U}_S(n) = \mathcal{U}_K^+$$

on $\mathcal{U}_K^+$ denota el grup de les unitats totalment positives de K.
Donat $j \in J(\Sigma)$, $j \neq 0$, 1728, considerem el conjunt:

$$\mathcal{M} = \{v \in \Sigma,\ v \not| 2,\ v(\Delta) \equiv 6 \pmod{12}\}.$$

Per a $v \in \Sigma$, definim $d_v \in K$ com:

$$d_v = \begin{cases} f(r) & \text{, si } v|2 \\ \pi & \text{, si } v \in \mathcal{M} \\ 1 & \text{, en altre cas} \end{cases}$$

on $r \in K$ és una arrel de $g(x)$ (mòdul $\pi^{2v(\Delta)/3}$).
Tenim els següents corol·laris:

COROL·LARI 2.3.1.
Per a $j \in J(\Sigma)$, $j \neq 0$, 1728, les següents afirmacions són equivalents:

(i) $j \in J$
(ii) *Existeix $d \in K$, satisfent:*

$$v(d) \equiv v(d_v) (mod\ 2) \qquad \forall v \in \Sigma\ i$$
$$d/d_v \equiv \alpha^2 (mod\ \pi^{2e+v(d/d_v)}),\ \alpha \in K, \qquad \forall v|2$$

(iii) $\prod_{v \in \Sigma} (d_v, u)_v = 1 \quad \forall u \in \mathcal{U}_K^+ / \mathcal{U}_K^2.$

DEMOSTRACIÓ:

Notem que $\mathcal{M}$ és precisament el conjunt de places, fora del 2, a les quals E_j té mala reducció (vegi's remarca 2.2.2). Es desprèn, també, de les remarques 2.2.2, 2.3.2, que $E_j^{d_v}$ té bona reducció a v, per a cada $v \in \Sigma$. Així, per la remarca 2.5.3, són equivalents:

(a) Existeix $d \in K$ tal que E_j^d té bona reducció arreu.
(b) $d_v/d \in H^1_{nr}(G_v, \mathbf{Z}/2\mathbf{Z})$.

Això prova l'equivalència entre les afirmacions (i) i (ii) del corol·lari.

L'equivalència entre (i) i (iii) s'obté directament del teorema 2.3 ∎

REMARCA 2.7:

Per les proposicions 2.1, 2.2, tenim que sempre:

$$0 \in J(\Sigma \backslash \{v \in \Sigma, v|3\}),\ 1728 \in J(\Sigma \backslash \{v \in \Sigma, v|2\}).$$

De fet,

$$0 \in J(\Sigma) \Longleftrightarrow K(\sqrt{-3})|K \text{ és no-ramificada a totes les places finites de } K.$$
$$1728 \in J(\Sigma) \Longleftrightarrow K(\sqrt{-1})|K \text{ és no-ramificada a totes les places finites de } K.$$

COROL·LARI 2.3.2.

Per a $1728 \in J(\Sigma)$, *tenim* $1728 \in J$ *si i sols si:*

$$\prod_{v|2} {}_4((\alpha+1)^2 - 1, u)_v = 1 \qquad \forall u \in \mathcal{U}_K^+/\mathcal{U}_K^4$$

on $\alpha \in K^*$ *satisfà:* $\alpha^2 + 1 \equiv 0$ *(mod 4).*

DEMOSTRACIÓ: És conseqüència directa del teorema 2.3 i la remarca 2.4.2 ∎

COROL·LARI 2.3.3.

Per a $0 \in J(\Sigma)$, *tenim* $0 \in J$ *si i sols si:*

$$\prod_{v|3} {}_3(2, u)_v \cdot {}_2(\pi^{e/2}, u)_v = 1, \qquad \forall u \in \mathcal{U}_K^+/\mathcal{U}_K^6$$

DEMOSTRACIÓ: És conseqüència del teorema 2.3 i la remarca 2.4.1. Per altra part, es té:

$${}_6(4\pi^{3e/2}, u)_v = {}_6(\pi^{3e/2}, u)_v \cdot {}_6(4, u)_v$$
$$\text{i } {}_6(\pi^{3e/2}, u)_v = {}_2(\pi^{e/2}, u)_v, \qquad {}_6(4, u)_v = {}_3(2, u)_v \text{ ∎}$$

CAPÍTOL III. ALGUNS RESULTATS EN COSSOS QUADRÀTICS.

Al llarg d'aquest capítol, seguirem la notació següent:
$K = \mathbb{Q}(\sqrt{m})$ serà un cos quadràtic amb discriminant:

$$M = \begin{cases} m, & \text{si } m \equiv 1 \pmod 4 \\ 4m, & \text{altrament.} \end{cases}$$

Posarem σ, l'automorfisme no trivial de K i

$$\varepsilon = \begin{cases} \text{la unitat fonamental}, & \text{si } m > 0 \\ \sqrt{-1}, & \text{si } m = -1 \\ (1+\sqrt{-3})/2, & \text{si } m = -3 \\ -1, & \text{si } m < 0,\ m \neq -1, -3. \end{cases}$$

També denotarem per H_K, H_K^+ els grups de classes d'ideals de K ample i estricte, respectivament, i h_K, h_K^+ seran els seus ordres respectius.

Finalment, utilitzarem la mateixa notació que en el Capítol II en quant a $J(v)$, $J(\Sigma)$, J, E_j, f, g, Δ, d_v i $\mathcal{M}$.

§1. Bona reducció i invariant j fixat.

El nostre objectiu, en aquesta secció, és donar una descripció més explícita que la del capítol anterior dels conjunts $J(\Sigma)$, J, quan el cos base és un cos quadràtic.

Abans, però, enunciem i demostrem un parell de lemes sobre unitats π-àdiques.

LEMA 3.1.

Suposem $p = 2$. Per a $u \in \mathcal{U}_v$ es té $u \in \mathcal{U}_v^2$ si i sols si es satisfà alguna de les condicions següents:

(i) $m \equiv 1 \pmod 8$, $u \equiv 1 \pmod{\pi^3}$.

(ii) $m \equiv 5 \pmod 8$, $u \equiv 1, 5, \dfrac{1 \pm \sqrt{m}}{2}, 5\left(\dfrac{1 \pm \sqrt{m}}{2}\right) \pmod{\pi^3}$.

(iii) $m \equiv 3 \pmod 4$, $u \equiv 1, m \pmod{\pi^5}$.

(iv) $m \equiv 2 \pmod 4$, $u \equiv 1, (1+\sqrt{m})^2 \pmod{\pi^5}$.

DEMOSTRACIÓ:

Quan $e = 1$ ($m \equiv 1 \pmod 4$), aleshores és ben conegut que $u \in \mathcal{U}_v^2$ si i sols si $u \equiv \alpha^2 \pmod{\pi^3}$, $\alpha \in \mathcal{U}_v$ (cf. [Bo-Sha], per exemple). D'aquesta darrera condició s'obtenen, per un càlcul directe, els resultats (i), (ii) de l'enunciat. Per això només cal posar:

$$\alpha \equiv s_1 + 2s_2 \pmod{\pi^2}, \qquad s_1 \not\equiv 0 \pmod \pi$$

on s_1, s_2 recorren un sistema complet S de residus mòdul π. Quan $m \equiv 1 \pmod 8$ prenem $S = \{0, 1\}$. Quan $m \equiv 5 \pmod 8$ prenem $S = \left\{0, 1, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}\right\}$.

Suposem, ara, $m \equiv 2, 3 \pmod 4$. Per a provar la suficiència de les condicions (iii), (iv), considerem el polinomi:

$$F(x) = x^2 - u$$

i sigui

$$x_0 = \begin{cases} 1, \sqrt{m}, & \text{segons } u \equiv 1, m \pmod{\pi^5} \text{ respect. i } m \equiv 3 \pmod 4 \\ 1, 1+\sqrt{m}, & \text{segons } u \equiv 1, 1+\sqrt{m} \pmod{\pi^5} \text{ respect. i } m \equiv 2 \pmod 4. \end{cases}$$

Aleshores,

$$F(x_0) \equiv 0 \pmod{\pi^5} \text{ i}$$
$$F'(x_0) = 2x_0 \not\equiv 0 \pmod{\pi^3}.$$

Per tant, existeix $\alpha \in \mathcal{U}_v$ tal que $\alpha \equiv x_0 \pmod{\pi^3}$ i $F(\alpha) = 0$.

Per a provar-ne la necessitat només cal desenvolupar la congruïtat

$$u \equiv \alpha^2 (\text{mod } \pi^5)$$

escrivint $\alpha \equiv 1 + s_1\pi + s_2\pi^2 \pmod{\pi^3}$, on $s_i \in \{0, 1\}$, $i = 1, 2$.

Notem, finalment, que podem prendre:

$$\pi = \begin{cases} 1+\sqrt{m} & \text{si } m \equiv 3 \pmod 4 \\ \sqrt{m} & \text{si } m \equiv 2 \pmod 4 \end{cases} \blacksquare$$

LEMMA 3.2.

Suposem $p \neq 2$ i sigui $u \in \mathcal{U}_v$ amb $N(u) \equiv 1 \pmod p$. Aleshores $u \in \mathcal{U}_v^2$ si i sols si es satisfà alguna de les condicions següents:

(i) $tr(u) \equiv 2 \pmod p$.
(ii) $tr(u) \equiv -2 \pmod p$, *p inert.*
(iii) $tr(u) \equiv -2 \pmod p$, *p no-inert*, $p \equiv 1 \pmod 4$.
(iv) $tr(u) \not\equiv \pm 2 \pmod p$, $tr(u) \pm 2 \in \mathbb{Z}_p^2$.

DEMOSTRACIÓ:

La propietat $u \in \mathcal{U}_v^2$ és equivalent a que la congruïtat:

$$u \equiv \alpha^2 (\text{mod } \pi)$$

tingui solució per a $\alpha \in \mathcal{O}_v$. De:

$$u^2 - tr(u)u + 1 \equiv 0 \pmod{p} \tag{3.1}$$

obtenim les dues congruïtats següents:

$$(u+1)^2 \equiv u(tr(u)+2) \pmod{p} \tag{3.2}$$

$$(u-1)^2 \equiv u(tr(u)-2) \pmod{p}. \tag{3.3}$$

Quan $tr(u) \equiv 2 \pmod{p}$, de (3.3) tenim:

$$u \equiv 1 \pmod{\pi}.$$

Quan $tr(u) \equiv -2 \pmod{p}$, de (3.2) tenim:

$$u \equiv -1 \pmod{\pi}.$$

Llavors, $-1 \equiv \alpha^2 \pmod{\pi}$. Observem que si p és inert l'anterior congruïtat sempre té solució, ja que si $\left(\frac{-1}{p}\right) = -1$ aleshores $\left(\frac{-m}{p}\right) = 1$ i, per tant, existirà $n \in \mathbb{N}$ tal que $(n\sqrt{m})^2 \equiv -1 \pmod{p}$.

Si p és no-inert, aleshores $\alpha \equiv a \pmod{\pi}$, $a \in \mathbb{N}$, i la congruïtat anterior té solució si i sols si $\left(\frac{-1}{p}\right) = 1$.

Podem suposar, doncs, $tr(u) \not\equiv \pm 2 \pmod{p}$.

La suficiència de les condicions (iv) és clara, a partir de (3.2), (3.3). Per a provar-ne la necessitat, podem escriure utilitzant les mateixes congruïtats:

$$\begin{aligned} tr(u) + 2 &\equiv \gamma^2 \pmod{p} \\ tr(u) - 2 &\equiv \eta^2 \pmod{p} \qquad \gamma, \eta \in \mathcal{U}_v \end{aligned}$$

d'aquí: $\gamma^2 \equiv (\gamma^\sigma)^2 \pmod{p}$, $\eta^2 \equiv (\eta^\sigma)^2 \pmod{p}$ i, per tant, $\gamma^\sigma \equiv \pm\gamma \pmod{\pi}$, $\eta^\sigma \equiv \pm\eta \pmod{\pi}$.

Observem que el cas $\gamma^\sigma \equiv -\gamma \pmod{\pi}$ i $\eta^\sigma \equiv -\eta \pmod{\pi}$ no es pot donar, ja que implicaria p inert i de $(\gamma\eta)^\sigma \equiv \gamma\eta \pmod{p}$ i la congruïtat:

$$(2u - tr(u))^2 \equiv tr(u)^2 - 4 \pmod{p}$$

tindriem $u \equiv a \pmod{p}$, $a \in \mathbb{N}$. Però així:

$$\begin{aligned} &N(u) \equiv a^2 \pmod{p}, \text{ per tant, } a \equiv \pm 1 \pmod{p} \text{ i} \\ &tr(u) \equiv \pm 2 \pmod{p} \ ! \end{aligned}$$

En tot altre cas, es satisfà (iv) ∎

TEOREMA 3.1.

Suposem $p = 3$, i sigui $j \in \mathcal{O}_v$, $j \neq 0, 1728$. Es té $j \in J(v)$ si i sols si es satisfà alguna de les condicions següents:

(i) $v(j) = 0$.
(ii) $v(j) = 3e$, $v(j - 1728) \geq 6e$, $v(j - 1728) \equiv 0$ *(mod 2).*
(iii) $3|m$, $j = 27u$ *i* $u \equiv 2$ *(mod* π^3*).*
(iv) $3|m$, $j = 3^{4+i}u$, $i \geq 0$, $i \not\equiv 1$ *(mod 3) amb:*

$$u \equiv \pm 4 \text{ (mod } \pi^3) \text{ si } i \equiv 2 \text{ (mod } 3)$$
$$6u \equiv \pm\pi^3 \text{ (mod } \pi^6) \text{ si } i \equiv 0 \text{ (mod } 3).$$

DEMOSTRACIÓ:

Pel corol·lari 2.1.3 del Capítol II, $j \in J(v)$ si i sols si es satisfà la condició (i), o la condició (ii) de l'enunciat, o bé una de les següents condicions:

(3.4) $e = 2$, $v(j) = 6$, $v(j - 1728) = 6$ i $f(x)$ té una arrel mòdul π^9.

(3.5) $e = 2$, $v(j) > 6$, $v(j) \equiv 0 \pmod 3$ i $f(x)$ té una arrel mòdul $\pi^{3+v(j)}$.

Anem a veure, primer, que la condició (3.4) és equivalent a (iii). En efecte:

De $f(x) \equiv 0 \pmod{\pi^9}$, $x \in \mathcal{O}_v$, tenim que $v(x) = 2$. Posem, doncs,

$$j = 27u, \qquad x = 3w, \qquad u, w \in \mathcal{O}_v.$$

Així, $v(j - 1728) = 6$ sii $u \equiv 2 \pmod \pi$. Podem escriure, per tant,

$$j = 27(2 + \lambda\pi), \qquad j - 1728 = 27(-62 + \lambda\pi), \qquad \lambda \in \mathcal{O}_v.$$

De $v\left(x^3 - \dfrac{54j}{j - 1728}\right) = 8$ es té:

$$v\left(w^3 - \frac{2(2 + \lambda\pi)}{-62 + \lambda\pi}\right) = 2$$

i d'aquí: $w \equiv 1 \pmod \pi$ o, equivalentment, $w^3 \equiv 1 \pmod{\pi^3}$.

Finalment, de $f(w, \lambda) \equiv 0 \pmod{\pi^9}$ obtenim $\lambda \equiv 0 \pmod{\pi^2}$.

Recíprocament, si es satisfà (iii) és immediat veure (refent els càlculs anteriors) que $f(3) \equiv 0 \pmod{\pi^9}$.

Tot seguit, vegem que la condició (3.5) és equivalent a (iv). En efecte, de $f(x) \equiv 0 \pmod{\pi^{3+v(j)}}$ tenim $v(x) = v(j)/3$. Posem, doncs,

$$j = 3^{4+i}u, \qquad i \geq 0, \qquad u \in \mathcal{O}_v$$

amb

$$v(u) = 0, \qquad i \equiv 2 \pmod 3, \text{ o bé,}$$
$$v(u) = 1, \qquad i \equiv 0 \pmod 3$$

i escrivim

$$x = \begin{cases} 3^{\frac{4+i}{3}} w,\ w \in \mathcal{O}_v,\ v(w) = 0, & \text{si } i \equiv 2 \pmod 3 \\ 3^{\frac{3+i}{3}} w,\ w \in \mathcal{O}_v,\ v(w) = 1, & \text{si } i \equiv 0 \pmod 3. \end{cases}$$

De la congruïtat:

$$x^3 - \frac{54j}{j - 1728} \equiv 0 \pmod{\pi^{3+v(j)}}$$

obtenim si $i \equiv 2 \pmod 3$:

$$w^3 \equiv \frac{2u}{3^{1+i}u - 64} \pmod{\pi^3}$$

i d'aquí, $2u \equiv -w^3 \equiv \pm 1 \pmod{\pi^3}$.

Mentre que quan $i \equiv 0 \pmod 3$:

$$w^3 \equiv \frac{6u}{3^{1+i}u - 64} \pmod{\pi^6}$$

i d'aquí $6u \equiv \pm\pi^3 \pmod{\pi^6}$.

Recíprocament, si es satisfà la condició (iv) és immediat comprovar que:

$$f(\mp 3^{\frac{4+i}{3}}) \equiv 0 \pmod{\pi^{3+v(j)}} \text{ si } i \equiv 2 \pmod 3$$
$$f(\mp 3^{\frac{3+i}{3}}\pi) \equiv 0 \pmod{\pi^{3+v(j)}} \text{ si } i \equiv 0 \pmod 3 \blacksquare$$

TEOREMA 3.2.

Suposem $p = 2$, i sigui $j \in \mathcal{O}_v$, $j \neq 0, 1728$. Es té $j \in J(v)$ si i sols si es satisfà alguna de les condicions següents:

(i) $v(j) = 0$.
(ii) $v(j) \geq 12e$, $v(j) \equiv 0$ *(mod 3)*.
(iii) $2|m$, $j - 1728 = 2^7 u$, *amb:*

$$v(2u + 4 + \pi^2) = 5, \text{ o bé, } v(2u + 4 - \pi^2) \geq 6.$$

(iv) $m \equiv 3$ *(mod 4)*, $j - 1728 = 2^{8+i}u$, $i \geq 0$, *amb:*

$$v(u \pm 1) = 3 \quad \text{si } i \equiv 0 \text{ (mod 2)},$$
$$v(2u \pm \pi^2) = 5 \quad \text{si } i \equiv 1 \text{ (mod 2)}.$$

DEMOSTRACIÓ:

Pel corol·lari 2.2.2 del Capítol II, $j \in J(v)$ si i sols is es satisfà la condició (i), o la condició (ii) de l'enunciat, o bé, la següent condició:

(3.6)

$e = 2$, $v(j) = 12$, $v(j-1728) \equiv 0 \pmod 2$ i $g(x)$ té una arrel mòdul $\pi^{32-2v(j-1728)}$.

Vegem que (3.6) és equivalent a les condicions (iii) i (iv) de l'enunciat. En efecte, considerem el polinomi:

$$\tilde{g}(x) := (j-1728)^4 \cdot 3^{-5} \cdot g\left(\frac{3x}{j-1728}\right) = x^4 - 6j(j-1728)x^2 - 8j(j-1728)^2x - 3j^2(j-1728)^2.$$

De $\tilde{g}(x) \equiv 0 \pmod{\pi^{32+2v(j-1728)}}$ tenim:

$$v(x) = 6 + v(j-1728)/2.$$

Podem escriure, doncs,

$$j - 1728 = 2^{7+i}u,\ i \geq 0,\ u \in \mathcal{U}_v$$
$$x = \pi^{13+i}w,\ w \in \mathcal{U}_v$$
$$2 = \pi^2\varepsilon,\ \varepsilon \in \mathcal{U}_v.$$

Expressem $\tilde{g}(x)$ de la següent manera:

$$\tilde{g}(x) = (x^2 - 3B)^2 - 12B^2 - 8B(j-1728)x$$

on $B = j(j-1728)$.

Així, $v(B) = 26 + 2i$, $v(\tilde{g}(x)) \geq 60 + 4i$.

Si $i \geq 1$, tenim:

$$(x^2 - 3B)^2 \equiv 12B^2 \pmod{\pi^{60+4i}}$$

i d'aquí $\left(\dfrac{x^2-3B}{2B}\right)^2 \equiv -1 \pmod{\pi^4}$.

Per tant, pel lema 3.1, hem de tenir necessàriament $m \equiv 3 \pmod 4$. Així

$$\frac{x^2-3B}{2B} \equiv 1 + \pi \pmod{\pi^2}$$

i d'aquí $v(x^2 - 5B) = 29 + 2i$.

Posant, doncs, $B = 2^{13+i}u(2^{1+i}u + 27)$ obtenim:

$$v(w^2 + \varepsilon^{13+i}u) = 3.$$

Si $i \equiv 1 \pmod 2$, de

$$v((w\varepsilon^{-\frac{13+i}{2}})^2 + u) = 3$$

i $(w\varepsilon^{-\frac{13+i}{2}})^2 \equiv \pm 1 \pmod{\pi^4}$ (lema 3.1) es desprèn que $v(u+1) = 3$ o $v(u-1) = 3$.

Si $i \equiv 0 \pmod 2$, de

$$v((w\varepsilon^{-\frac{12+i}{2}})^2 + \varepsilon u) = 3$$

tenim

$$v((\pi w\varepsilon^{-\frac{12+i}{2}})^2 + 2u) = 5$$

on, ara, $(\pi w\varepsilon^{-\frac{12+i}{2}})^2 \equiv \pm\pi^2 \pmod{\pi^6}$.

S'obtenen, així, les condicions (iv).

Per a provar el recíproc, sols cal refer el procés anterior, per a trobar una arrel x del polinomi $\tilde{g}(x)$. És immediat comprovar que per:

$$x = \begin{cases} 2^{\frac{13+i}{2}} & \text{si } i \equiv 1(\text{mod } 2), \quad v(u+1) = 3 \\ 2^{\frac{13+i}{2}}\sqrt{m} & \text{si } i \equiv 1(\text{mod } 2), \quad v(u-1) = 3 \\ 2^{\frac{12+i}{2}}\pi & \text{si } i \equiv 0(\text{mod } 2), \quad v(2u+\pi^2) = 5 \\ 2^{\frac{12+i}{2}}\pi\sqrt{m} & \text{si } i \equiv 0(\text{mod } 2), \quad v(2u-\pi^2) = 5 \end{cases}$$

es té $\tilde{g}(x) \equiv 0 \pmod{\pi^{32+2(j-1728)}}$.

Finalment, considerem el cas $i = 0$.

De $\tilde{g}(x) \equiv 0 \pmod{\pi^{60}}$ tenim:

$$v((x^2 - 3B)^2 - 12B^2) = v(8B(j-1728)x) = 59$$

i d'aquí, posant $B = \varepsilon^{13}\pi^{26}u(2u+27)$ tenim:

$$v((w^2 - 3\varepsilon^{13}u(2u+27))^2 + 4\varepsilon^{26}u^2(2u+27)^2) = 7 \tag{3.7}$$

i, en conseqüència,

$$v(w^2 - 3\varepsilon^{13}u(2u+27)) = 2.$$

Posant $w^2 = 2\lambda + 3\varepsilon^{13}u(2u+27)$, $\lambda \in \mathcal{U}_v$ i substituint a (3.7) obtenim:

$$v(\lambda^2 + \varepsilon^{26}u^2(2u+27)^2) = 3.$$

Pel lema 3.1, necessàriament, $d \equiv 2 \pmod 4$.

Si posem $\lambda = \varepsilon^{13}u(2u+27) + \alpha\pi$, $\alpha \in \mathcal{U}_v$ aleshores,

$$w^2 = 2\pi\alpha + 5\varepsilon^{13}u(2u+27).$$

Per tant,

$$v(w^2 - 5\varepsilon^{13}u(2u+27)) = 3$$

o, equivalentment,

$$v((\pi w\varepsilon^{-6})^2 + 2u + 4) = 5.$$

Però de $v((w\varepsilon^{-6})^2 - 1) \geq 4$ o $v((w\varepsilon^{-6})^2 + 1) = 3$ (lema 3.1) es té:

$$v(2u + 4 + \pi^2) = 5 \text{ o } v(2u + 4 - \pi^2) \geq 6, \text{ respectivament.}$$

S'obté, així, la condició (iii) del teorema.

Pel recíproc, només cal comprovar que quan

$$x = \begin{cases} 2^6\pi & \text{si } v(2u + 4 + \pi^2) = 5 \\ 2^6\pi(1 + \sqrt{m}) & \text{si } v(2u + 4 - \pi^2) \geq 6 \end{cases}$$

aleshores $\tilde{g}(x) \equiv 0 \pmod{\pi^{60}}$ ∎

REMARQUES 3.2:

En la demostració del teorema 3.2 s'ha provat que:

(1) Si $j \in J(v)$ satisfà la condició (iii) del teorema 3.2, aleshores una arrel $r \in K$ de $g(x)$ (mòdul $\pi^{2v(\Delta)/3}$) és:

$$r = \begin{cases} \dfrac{3\pi}{2u} & \text{si } v(2u + 4 + \pi^2) = 5 \\ \dfrac{3\pi}{2u}(1 + \sqrt{m}) & \text{si } v(2u + 4 - \pi^2) \geq 6. \end{cases}$$

(2) Si $j \in J(v)$ satisfà la condició (iv) del teorema 3.2, aleshores una arrel $r \in K$ de $g(x)$ (mòdul $\pi^{2v(\Delta)/3}$) és:

$$r = \begin{cases} \dfrac{3}{2^{\frac{2+i}{2}}u} & \text{si } i \equiv 0 (\text{mod } 2), \quad v(u + 1) = 3 \\ \dfrac{3\sqrt{m}}{2^{\frac{2+i}{2}}u} & \text{si } i \equiv 0 (\text{mod } 2), \quad v(u - 1) = 3 \\ \dfrac{3\pi}{2^{\frac{3+i}{2}}u} & \text{si } i \equiv 1 (\text{mod } 2), \quad v(2u + \pi^2) = 5 \\ \dfrac{3\pi}{2^{\frac{3+i}{2}}u}\sqrt{m} & \text{si } i \equiv 1 (\text{mod } 2), \quad v(2u - \pi^2) = 5. \end{cases}$$

COROL·LARI 3.2.1.

Per a $j \in K$, $j \neq 0$, 1728, es té $j \in J(\Sigma)$ si i sols si :

(a) $v(j) \geq 0$, $v(j) \equiv 0$ *(mod 3)*, $v(j - 1728) \equiv 0$ *(mod 2) per a tot* $v \in \Sigma$.

(b) *Per a $p = 3$ i $v(j) > 0$ es satisfà alguna de les condicions següents:*

(i) $v(j - 1728) \geq 6e$.

(ii) $3|m$, $j = 27(x + y\sqrt{m})/2$, $x \equiv 4$ *(mod 9)*, $y \equiv 0$ *(mod 3)*.
(iii) $3|m$, $j = 3^{4+i}(x + y\sqrt{m})/2$, $i \geq 0$, $i \not\equiv 1$ *(mod 3)*, amb:

$$x \equiv \pm 1 \text{ (mod 9)}, \ y \equiv 0 \text{ (mod 3)}, \text{ si } i \equiv 2 \text{ (mod 3)}$$
$$x \equiv 0 \text{ (mod 9)}, \ y \equiv \pm\frac{m}{3} \text{ (mod 9)}, \text{ si } i \equiv 0 \text{ (mod 3)}.$$

(c) *Per a* $p = 2$ *i* $v(j) > 0$ *es satisfà alguna de les condicions següents:*
(i) $v(j) \geq 12e$.
(ii) $2|m$, $j - 1728 = 2^7(x + y\sqrt{m})$, $y - x \equiv \frac{m}{2}$ *(mod 4)*, $y \equiv 0$ *(mod 2)*.
(iii) $m \equiv 3$ *(mod 4)*, $j - 1728 = 2^{8+i}(x + y\sqrt{m})$, $i \geq 0$, amb:

$$x \equiv (m-3)/2 \text{ (mod 4)}, \ y \equiv 1 \text{ (mod 2)}, \text{ si } i \equiv 1 \text{ (mod 2)}$$
$$x \equiv 1 \text{ (mod 2)}, \ y \equiv 2 \text{ (mod 4)}, \text{ si } i \equiv 0 \text{ (mod 2)}.$$

DEMOSTRACIÓ:
La condició b (ii) s'obté del teorema 3.1, (iii) en fer:

$$N(x - 4 + y\sqrt{m}) \equiv 0 \text{ (mod 27)}.$$

Semblantment, la condició b (iii) s'obté de (iv) del teorema 3.1, posant:

$$N(x \pm 8 + y\sqrt{m}) \equiv 0 \text{ (mod 27) quan } i \equiv 2 \text{ (mod 3)}$$
$$\text{i } 3(x + y\sqrt{m}) \equiv \pm m\sqrt{m} \text{ quan } i \equiv 0 \text{ (mod 3)}.$$

Finalment, les condicions c (ii), c (iii), resulten del teorema 3.2 (iii), (iv), procedint com segueix:
Quan $2|m$, prenem $\pi = \sqrt{m}$. Aleshores de

$$(2x + m + 4)^2 - 4y^2 m \equiv 0 \text{ (mod 32)}$$

tenim:

$$y \equiv 2 \text{ (mod 4)}$$
$$x + 2 \equiv \frac{-m}{2} \text{ (mod 4)}.$$

Per altra part, de $2x + 4 - m + 2y\sqrt{m} \equiv 0$ (mod 8) tenim:

$$y \equiv 0 \text{ (mod 4)},$$
$$x + 2 \equiv \frac{m}{2} \text{ (mod 4)}.$$

Quan $2 \nmid m$, prenem $\pi = 1 + \sqrt{m}$.
Si $i \equiv 0 \pmod 2$, de

$$(x \pm 1)^2 - y^2 m \equiv 0 \pmod 8$$

tenim:

$$x \equiv \pm 1 \pmod 4,\ y \equiv 2 \pmod 4.$$

Si $i \equiv 1 \pmod 2$, de

$$(2x \pm (1+m))^2 - (2y \pm 2)^2 m \equiv 0 \pmod{32}$$

tenim:

$$y \pm 1 \equiv 2 \pmod 4$$
$$x + \frac{1+m}{2} \equiv 2 \pmod 4 \blacksquare$$

REMARQUES 3.2.3:
De la demostració del corol·lari 3.2.1 i les remarques 3.2 obtenim:

(i) Si $j \in J(v)$ satisfà la condició c (ii) del corol·lari 3.2.1, aleshores una arrel $r \in K$ de $g(x)$ (mòdul $\pi^{2v(\Delta)/3}$) és:

$$r = \begin{cases} \dfrac{3\sqrt{m}}{2(x + y\sqrt{m})} & \text{si } y \equiv 2 \pmod 4 \\ \dfrac{3(m+\sqrt{m})}{2(x+y\sqrt{m})} & \text{si } y \equiv 0 \pmod 4. \end{cases}$$

(ii) Si $j \in J(v)$ satisfà la condició c (iii) del corol·lari 3.2.1, aleshores una arrel $r \in K$ de $g(x)$ (mòdul $\pi^{2v(\Delta)/3}$) és:

$$r = \begin{cases} \dfrac{3}{2^{\frac{2+i}{2}}(x + y\sqrt{m})} & \text{si } i \equiv 0 \pmod 2, \quad x \equiv 1 \pmod 4 \\ \dfrac{3\sqrt{m}}{2^{\frac{2+i}{2}}(x + y\sqrt{m})} & \text{si } i \equiv 0 \pmod 2, \quad x \equiv 3 \pmod 4 \\ \dfrac{3(1+\sqrt{m})}{2^{\frac{3+i}{2}}(x + y\sqrt{m})} & \text{si } i \equiv 1 \pmod 2, \quad y \equiv 1 \pmod 4 \\ \dfrac{3(m+\sqrt{m})}{2^{\frac{3+i}{2}}(x + y\sqrt{m})} & \text{si } i \equiv 1 \pmod 2, \quad y \equiv 3 \pmod 4. \end{cases}$$

DEFINICIÓ: Sigui K amb $N(\varepsilon) = 1$. Donat un primer $p \in \mathbb{N}$, $p \neq 2$, direm que p satisfà la condició $(*)$ si i sols si:

(1) $p \not| (tr(\varepsilon) - 2)$.
(2) Si $p | (tr(\varepsilon) + 2)$ aleshores p és no-inert, $p \equiv 3 \pmod 4$.
(3) Si $p \not| (tr(\varepsilon) + 2)$ aleshores $\left(\frac{tr(\varepsilon)+2}{p}\right) = \left(\frac{tr(\varepsilon)-2}{p}\right) = -1$.

Notarem per:

$$\Sigma^* := \{v \in \Sigma,\ v \not| 2,\ \text{tals que } p \text{ satisfà la condició } (*)\}.$$

TEOREMA 3.3.
Per a $j \in J(\Sigma)$, $j \neq 0, 1728$, són equivalents:

(i) $j \in J$.

(ii) *Existeix $d \in K$ amb $|N(d)| = N\left(\sum_{v\in\Sigma} v(d_v) \cdot v\right)$ i tal que*

$$\frac{d}{f(r)} \equiv \alpha^2 \ (mod\ 4)\ ,\ \alpha \in K,\ (\alpha, 2) = 1.$$

(iii) *$N(\varepsilon) = -1$, o bé, $N(\varepsilon) = 1$ i es satisfà:*

$$\#(\mathcal{M} \cap \Sigma^*) \equiv \sum_{v\in\Sigma^*} v(f(r))\ (mod\ 2).$$

DEMOSTRACIÓ:
Pel corol·lari 2.3.1 (Capítol II), (i) és equivalent a l'existència de $d \in K$ tal que:

$$(d) = \left(\sum_{v\in\Sigma} v(d_v) \cdot v\right) \mathcal{B}^2,$$

per a un cert ideal $\mathcal{B}$ de K, i

$$\frac{d}{f(r)} \equiv \alpha^2 (\text{mod } \pi^{2e+v(\frac{d}{f(r)})})$$

per a tot $v|2$, $\alpha \in K$. Podem suposar $(\mathcal{B}, 2) = 1$. Per tant, $v\left(\frac{d}{f(r)}\right) = 0$, per a tot $v|2$.

Finalment, la primera condició és equivalent a que l'ideal $\left(\sum_{v\in\Sigma} v(d_v) \cdot v\right)$ sigui del gènere principal.

També pel corol·lari 2.3.1, la condició (i) resulta ésser equivalent a:

$$\prod_{v\in\Sigma}(d_v,u)_v = 1 \text{ per a tot } u \in \mathcal{U}_K^+/\mathcal{U}_K^2.$$

Ara, però,

$$\frac{\mathcal{U}_K^+}{\mathcal{U}_K^2} = \begin{cases} \{1\} & \text{si } N(\varepsilon) = -1\,(m>0) \\ \{1,\varepsilon\} & \text{si } N(\varepsilon) = 1. \end{cases}$$

Quan $N(\varepsilon)=1$, observem que per $v\in\Sigma$, $v\nmid 2$ tenim:

$$(d_v,\varepsilon)_v = \begin{cases} (-1)^{v(d_v)} & \text{si } \varepsilon \notin \mathcal{U}_v^2 \\ 1 & \text{en altre cas.} \end{cases}$$

Per tant, pel lema 3.2:

$$\prod_{v\in\Sigma}(d_v,\varepsilon)_v = 1 \Longleftrightarrow \prod_{v|2}(f(r),\varepsilon)_v = (-1)^{\#(\mathcal{M}\cap\Sigma^*)}.$$

Però, per altra part, de $\prod_{v\in\Sigma}((f(r),\varepsilon)_v = 1$ es té:

$$\prod_{v|2}(f(r),\varepsilon)_v = \prod_{v\in\Sigma^*}(f(r),\varepsilon)_v.$$

Això acaba la demostració ∎

EXEMPLE 1:

Sigui K un cos de nombres arbitrari i suposem que $(h_K,6)=1$. En aquest cas, tota corba el·líptica amb bona reducció arreu ha de tenir un model minimal global [cf. Set1]. Considerem els invariants c_4, c_6 d'un tal model de Weierstraß. Aleshores satisfan la següent relació:

$$c_4^3 - c_6^2 = 1728u, \qquad u\in\mathcal{U}_K.$$

Per tant, el problema de determinar el conjunt de les corbes el·líptiques sobre K amb bona reducció arreu és equivalent a trobar les solucions enteres (x,y) de les equacions el·líptiques:

$$y^2 = x^3 - 1728u, \qquad u\in\mathcal{U}_K \tag{3.8}$$

tals que x, y puguin ésser realitzades com els invariants c_4, c_6 d'alguna equació de Weierstraß sobre $\mathcal{O}_K$.

Donada una d'aquestes solucions, la corba el·líptica corresponent tindria invariant $j = x^3u^{-1}$. De fet, aquest problema és equivalent al de la descripció de J.

Més concretament, quan K és un cos quadràtic es té el següent resultat:

Sigui (x,y) una solució entera de (3.8). Aleshores, x, $\pm y$ poden ésser realitzats com els invariants c_4, c_6 d'una corba el·líptica sobre $\mathcal{O}_K$ si i sols si $u^{-1}x^3 \in J$ -és a dir, $u^{-1}x^3$ satisfà les condicions del corol·lari 3.2.1 i el teorema 3.3-. En aquest cas, una manera de determinar el signe de y és la següent:

y en podrà ésser realitzat com l'invariant c_6 si i sols si:

$$\frac{xy}{f(r)} \equiv \alpha^2 \ (mod\ \pi^{2e+v(\frac{xy}{f(r)})}), \qquad \alpha \in K$$

per a tot $v|2$.

DEMOSTRACIÓ:

Pels resultats de Setzer [cf. Set2], es té $j \neq 0, 1728$. Sigui $E|K$ amb b.r.a. tal que:

$$c_4(E) = x, \qquad c_6(E) = y.$$

Aleshores $j(E) = u^{-1}x^3$, $\gamma(E) \equiv -c_4c_6$. Per tant, com que $\gamma(E_j) \equiv -1$,

$$E_j^{c_4c_6} \cong E.$$

Així, $j(E) \in J$ i $\frac{c_4c_6}{d_v} \in H^1_{nr}(G_v, \mathbb{Z}/2\mathbb{Z})$ per a tot $v \in \Sigma$. D'aquí en surt la necessitat de les condicions.

Recíprocament, sigui E amb b.r.a. (i model minimal global) tal que $j(E) = u^{-1}x^3$.

Posem $\Delta(E) = v$, $v \in \mathcal{U}_K$. Aleshores:

$$c_4^3 = u^{-1}vx^3, \text{ d'on } u^{-1}v \in \mathcal{U}_K^3$$
$$c_6^2 = u^{-1}vy^2, \text{ d'on } u^{-1}v \in \mathcal{U}_K^2.$$

Així, doncs, $u^{-1}v \in \mathcal{U}_K^6$. Posem $u^{-1}v = w^6$, $w \in \mathcal{U}_K$. Tenim:

$$c_4 = \mu \cdot w^2x, \text{ on } \mu^3 = 1$$
$$c_6 = w^3y.$$

Però com que a $\mathbb{Q}(\sqrt{-3})$ no hi ha corbes el·líptiques amb conductor trivial [cf. Stro] hem de tenir $\mu = 1$.

Finalment, de $\frac{xy}{f(r)}, \frac{c_4c_6}{f(r)} \in H^1_{nr}(G_v, \mathbb{Z}/2\mathbb{Z})$ $\forall v|2$ en resulta $w \in H^1_{nr}(G_v, \mathbb{Z}/2\mathbb{Z})$ $\forall v \in \Sigma$.

Per tant, $E^{w^{-1}}$ tindrà b.r.a. i un model minimal global amb:

$$c_4(E^{w^{-1}}) = x, \qquad c_6(E^{w^{-1}}) = y \blacksquare$$

EXEMPLE 2.

Sigui $j \in \mathcal{O}_K$, $j \neq 0$ i tal que $tr(j) = 0$, aleshores $j \notin J(\Sigma)$.

DEMOSTRACIÓ:

Hem de veure que no es satisfan les condicions del corol·lari 3.2.1. En primer lloc, observem que:

$$v(j) \equiv 0 \pmod 3 \ \forall v \in \Sigma \Longleftrightarrow j = (n\sqrt{m})^3, \qquad n \in \mathbb{Z}.$$

En efecte, si $v(j) \equiv 0 \pmod 3$ $\forall v \in \Sigma$ aleshores $N(j) \in \mathbb{Z}^3$, per tant, existeix $n \in \mathbb{Z}$ tal que $j = n^3 m\sqrt{m} = (n\sqrt{m})^3$.

Vegem, ara, que $(j, 3) = 1$. En efecte, la condició b (i) del corol·lari no es satisfà ja que la congruïtat:

$$j - 1728 \equiv 0 \pmod{3^6}$$

implicaria $1728 \equiv 0 \pmod{3^6}$!.

La condició b (ii) tampoc es satisfà, per ésser $tr(j) = 0$. Finalment, la condició b (iii) implicaria:

$$j = 3^{4+i} \cdot n_1^3 \cdot \frac{m}{3}\sqrt{m}, \qquad i \equiv 0 (\mathrm{mod}\ 3), \qquad (n_1, 3) = 1$$

i

$$n_1^3 \cdot \frac{m}{3} \equiv \pm\frac{m}{6} \pmod 9$$

la qual cosa és contradictòria, ja que $n_1^3 \equiv \pm 1 \pmod 9$.

En quant als primers dividint 2, es té per $v \in \Sigma$, $v|2$:

$$v(j) > 0 \Longleftrightarrow 2|j \Longleftrightarrow 16|n.$$

En efecte, l'única possibilitat és que $2^{12}|j$. La condició c (ii) no es dóna ja que $tr(j) = 0$ i la condició c (iii) implicaria: $1728 \equiv 0 \pmod{2^{8+i}}$!.

Seguidament estudiem la congruïtat:

$$v(j - 1728) \equiv 0 \pmod 2 \ \forall v \in \Sigma.$$

Notem que aquesta es satisfà sii $|N(j - 1728)| \in \mathbb{Z}^2$. En efecte, l'únic que cal estudiar és l'exponent dels primers inerts que divideixen $j - 1728$, però els únics possibles són $p = 2, 3$. Pels arguments anteriors concloem que $3 \not| j - 1728$ i que si $2|j - 1728$ llavors ho fa amb potència exactament 6.

Finalment, provarem que l'equació:

$$x^3 - (1728)^2 = \pm y^2, \qquad x, y \in \mathbb{Z} \tag{3.9}$$

amb $(x, 3) = 1$ i $2|y \Longrightarrow 2^6 \| y$, no té cap solució.

Suposem, primer, $(y, 2) = 1$. De la factorització:

$$[x - (12)^2][(x - (12)^2)^2 + 3(12)^2 x] = \pm y^2$$

tenim que l'equació (3.9) és equivalent al sistema:

$$\begin{cases} x - (12)^2 = \pm y_1^2 \\ (x - (12)^2)^2 + 3(12)^2 x = \pm y_2^2 \end{cases}$$

substituint s'obté l'equació:

$$y_1^4 \pm 3(12)^2 y_1^2 + 3(12)^4 \mp y_2^2 = 0.$$

Imposant que el discriminant ha d'ésser un quadrat s'obté:

$$-3(12)^4 + 4y_2^2 = (2A)^2, \qquad A \in \mathbb{Z} \tag{3.10}$$

i així,

$$2y_1^2 = \mp 3(12)^2 \pm 2A. \tag{3.11}$$

És un senzill càlcul comprovar que (3.10) només té les següents solucions:

$$(y_2 = \pm 259), \qquad A = \pm 227$$

i cap d'elles satisfà (3.11) per algun y_1.

Suposem, finalment, $2|y$. Dividint l'equació (3.9) per 2^{12} s'obté una nova equació:

$$x^3 - (27)^2 = \pm y^2, \qquad x, y \in \mathbb{Z}$$

amb $(x, 3) = (y, 2) = 1$.

Factorizant-la, la convertim en l'equivalent sistema:

$$\begin{cases} x - 9 = \pm y_1^2 \\ (x - 9)^2 + 27x = \pm y_2^2 \end{cases}$$

i procedint com abans s'obté:

$$-243 + 4y_2^2 = A^2, \qquad A \in \mathbb{Z} \tag{3.12}$$

$$2y_1^2 = \mp 27 \pm A. \tag{3.13}$$

Es comprova fàcilment que (3.12) només admet com a solucions:

$$(y_2 = \pm 61), \qquad A = \pm 121$$

amb cap de les quals es pot satisfer (3.13) ∎

EXEMPLE 3:

Sigui $j \in \mathbb{Z}$, $j \neq 0, 1728$. Aleshores:

(a) $j \in J(\Sigma)$ si i sols si $j = n^3$, $j - 1728 \in D \cdot \mathbb{Z}^2$, n, $D \in \mathbb{Z}$ i tals que:
  (i) $D|M$.
  (ii) Si $3|n$ llavors $27|n - 12$.
  (iii) Si $2|n$ llavors $16|n$, o bé, $16|n - 4$, $2|D$ i $D = m + 4 \pmod 8$.

(b) Per a $j \in J(\Sigma)$, $j \neq 0, 1728$, tenim $j \in J$ si i sols si:
  (i) $m \equiv 5 \pmod 8$, quan $D \equiv \pm 3 \pmod 8$.
  (ii) δD és una norma a K, on $\delta = \pm 1$ i $\delta D \equiv 1 \pmod 4$, quan $2 \not| D$.
  (iii) $-D$ és una norma a K, quan $2|D$.

Aquests resultats ja foren obtinguts per Setzer [cf. Set2]. Nosaltres en donem la demostració següent,

DEMOSTRACIÓ:

Les afirmacions de (a) són conseqüència immediata del corol·lari 3.2.1. Posem:

$$n^3 - 1728 = (n - 12)((n - 12)^2 + 36n).$$

Vegem que si $3|n$, les possibilitats b (ii), b (iii) del corol·lari 3.2.1 no es podem donar, perquè en qualsevol cas impliquen $j \notin \mathbb{Z}^3$. Per tant, per b (i) $3^6|n^3 - 1728$, o equivalentment, $3^3|n - 12$.

Quan $2|n$, la possibilitat c (iii) tampoc es dóna, ja que implicaria $j \notin \mathbb{Z}$.

Per a provar les afirmacions de (b), cal observar, en primer lloc, que si $v \in \Sigma$ satisfà $v(D) > 0$ aleshores $v(\Delta) \equiv 6 \pmod{12}$ i, per tant, $v(d_v) \equiv 1 \pmod 2$. Mentre que, per a $v|M$ i tal que $v(D) = 0$ es té $v(d_v) \equiv 0 \pmod 2$. Observem també que de $j \in \mathbb{Z}$ sempre es té: $v(d_v) \equiv v^\sigma(d_{v^\sigma}) \pmod 2$ $\forall v \in \Sigma$.

Per tant, per la condició (ii) del teorema 3.3, existeix un element $t \in K$ amb $N(t) = \pm D$, i tal que $d = ta$, $a \in \mathbb{Z}$. Llavors, de:

$$\frac{d}{f(r)} \equiv \alpha^2 \pmod 4, \qquad \alpha \in K, \qquad (\alpha, 2) = 1$$

prenent normes obtenim:

(1) Si $2 \not| D$, per a (iii), i la remarca 2.3.2 del Capítol II, podem prendre:

$$f(r) = \begin{cases} -1, & \text{si } 2 \not| n \\ \dfrac{-6}{j - 1728}, & \text{si } 2|n. \end{cases}$$

Per tant, $N(t) \equiv 1 \pmod 4$.

(2) Si $2|D$ estem, com hem vist, en la possibilitat c (ii) del corol·lari 3.2.1. Per les remarques 3.2.1, una arrel r de $f(x)$ és:

$$r = \frac{3(m+\sqrt{m})}{2x}, \qquad x \equiv -\frac{m}{2} \pmod 4$$

on $j - 1728 = 2^7 x$.

És un càlcul senzill veure que:

$$v(f(r)) = -1, \qquad v|2.$$

Per tant, $N\left(\frac{1}{f(r)}\right) \equiv 2 \pmod 4$ i, a més,

$$tr\left(\frac{1}{f(r)}\right) = \frac{tr(f(r))}{N(f(r))} \equiv 2 \pmod 4.$$

Així doncs, com que $m \equiv D + 4 \pmod 8$ tenim:

$$N\left(\frac{1}{f(r)}\right) \equiv -D \pmod 8.$$

Això prova la condició b (iii) de l'enunciat.

El recíproc és clar a partir de la següent propietat:
La congruïtat $x \equiv \pm\alpha^2 \pmod 4$, x, $\alpha \in K$, $(\alpha, 2) = 1$ té solució sii:

$$N(x) \equiv 1 \pmod 8 \text{ i: } (m,2) = 1,\ m \not\equiv 5 \pmod 8.$$
$$N(x) \equiv 1 \pmod 4 \text{ i: } 2|m \text{ ó } m \equiv 5 \pmod 8) \blacksquare$$

§2. Bona reducció i model minimal global.

Ens interessa, en aquesta secció, respondre la següent qüestió:
Donada una corba el·líptica sobre K, amb bona reducció arreu, existeix un torcement quadràtic seu amb bona reducció arreu i model minimal global?.

Abans d'envestir directament aquest problema, ens serà útil recordar el concepte de classe de Weierstraß d'una corba el·líptica, així com algunes de les seves propietats. En tot el que immediatament seguirà podem suposar K un cos de nombres arbitrari.

Sigui E una corba el·líptica sobre K. Per a cada valoració $v \in \Sigma$, considerem un model v-minimal de E, amb discriminant Δ_v i diferencial ω_v. Aleshores, el discriminant minimal de E, $\mathcal{D}(E|K)$, és l'ideal associat al divisor $\sum_{v\in\Sigma} v(\Delta_v)\cdot v$.

Sigui, ara, una equació de Weierstraß afí de E, arbitrària:

$$F(x,y) = 0$$

amb discriminant Δ_F i diferencial ω_F; i considerem el divisor:

$$A_F = \sum_{v \in \Sigma} v\left(\frac{\omega_F}{\omega_v}\right) \cdot v.$$

Aleshores és fàcilment verificable que:

(i) Classe $(A_F) \in H_K$ és independent de F.
(ii) Classe $(12A_F) =$ Classe $(\mathcal{D}(E|K))$.

Posem $a(E|K) :=$ classe (A_F). $a(E|K)$ s'anomena la classe de Weierstraß de E sobre K.

REMARQUES 3.3.1:

(i) Vegi's l'article de Silverman [Sil1] per una construcció de $a(E|K)$ equivalent.
(ii) Observem que $v\left(\frac{\omega_F}{\omega_v}\right) = \frac{1}{12} v\left(\frac{\Delta_v}{\Delta_F}\right)$ per a tot $v \in \Sigma$.
Per tant, si E té bona reducció arreu, llavors:

$$A_F = \sum_{v \in \Sigma} -\frac{1}{12} v(\Delta_F) \cdot v.$$

En aquest cas, tenim també, $a(E|K)^{12} = 1$.

La classe de Weierstraß de $E|K$ ens caracteritza l'existència d'un model minimal global sobre K, per a E, en el següent resultat:

TEOREMA ([SET1]).
$E|K$ admet un model minimal global si i sols si $a(E|K) = 1$.

Com a corol·lari immediat, Setzer obté el següent resultat que respon parcialment a la qüestió que inicialment hem formulat:

COROL·LARI ([SET1]).
Suposem $(h_K, 6) = 1$. Aleshores si E té bona reducció arreu sobre K, E ha de tenir un model minimal global.

Sigui E^χ el torcement quadràtic de E, associat a $d \in K^*/K^{*^2}$. Volem relacionar les classes $a(E|K)$ i $a(E^\chi|K)$.

Per això, sigui $F(x,y) = 0$ una equació de Weierstraß de E tal que $a_1 = a_3 = 0$. Llavors,

$$F^\chi(x,y) = x^3 + a_2 d x^2 + a_4 d^2 x + a_6 d^3 - y^2 = 0$$

és una equació de Weierstraß per a E^χ i es té:

$$\Delta_{F\chi} = d^6 \Delta_F.$$

Per tant,

$$\begin{aligned} A_{F\chi} - A_F &= \sum_{v\in\Sigma} \frac{1}{12}[v(\Delta_v^\chi) - v(\Delta_v) + v(\Delta_F) - v(\Delta_{F\chi})] \cdot v \\ &= \sum_{v\in\Sigma} \frac{1}{12}[-12h_v + 6\delta(d) - 6v(d)] \cdot v \\ &= \sum_{v\in\Sigma} \frac{1}{2}[\delta(d) - v(d)] \cdot v - \sum_{v\in\Sigma} h_v \cdot v. \end{aligned}$$

Notem per $a(\chi) :=$ classe $\left(\sum_{v\in\Sigma} \frac{1}{2}[\delta(d) - v(d)] \cdot v\right)$.

Observem que $a(\chi)$ és justament la classe de Steinitz de $K(\sqrt{d})$ respecte de K, tal i com la definiren Artin [Ar] i Fröhlich [Frö]. En efecte, es té la següent igualtat:

$$\mathcal{D}(\chi) = \left(\sum_{v\in\Sigma} \frac{1}{2}[\delta(d) - v(d)] \cdot v\right)^2 (d).$$

Obtenim, per tant, la següent relació entre les classes de Weierstraß de E i de E^χ:

$$a(E^\chi|K) = a(E|K) \cdot a(\chi) \cdot \text{classe } (\eta) \tag{3.14}$$

on $\eta = \left(\sum_{v\in\Sigma} h_v \cdot v\right)$, essent $(h_v)_{v\in\Sigma}$ els factors de correcció local de la fórmula dels discriminants minimals (vegi's Capítol I).

Recordem, finalment, dues propietats importants de la classe de Steinitz:

(i) $a(\chi) = 1$ sii l'extensió $K(\sqrt{d})|K$ admet una base entera (és a dir, si $\mathcal{O}_L$ és un $\mathcal{O}_K$-mòdul lliure).

(ii) Donada $c \in H_K$, existeix χ tal que:

$$a(\chi) = c.$$

Aquesta darrera propietat fou provada per Fröhlich [Frö], la demostració del qual és constructiva, i el caràcter χ corresponent resulta ser sempre ramificat sobre els primers que divideixen 2 i sobre un altre primer.

De fet, Silverman [Sil1] prova que es pot modificar la demostració de Fröhlich, per a construir un caràcter χ no-ramificat sobre un conjunt finit de primers prefixat. En aquest mateix treball, Silverman utilitza la propietat (ii) de la classe de Steinitz per a demostrar el resultat següent:

TEOREMA ([SIL1]).

Sigui $c \in H_K$. Donada una corba el·líptica $E|K$, existeix un torcement quadràtic E^χ de E amb classe de Weierstraß:

$$a(E^\chi|K) = c.$$

En particular, donada una corba el·líptica sobre K amb bona reducció arreu, existeix sempre un torcement amb model minimal global però, de entrada, no es té cap control sobre la reducció d'aquest torcement.

Tornem, ara, al plantejament inicial d'aquesta secció, on $K = \mathbb{Q}(\sqrt{M})$ és un cos quadràtic de discriminant M. Prèviament, però, necessitem estudiar les extensions quadràtiques de K no-ramificades als primers finits:

Extensions discriminantals de K.

És elemental veure que M factoritza de manera única com a producte de discriminants primers, entenent per discriminant primer un nombre enter del següent tipus:

$$(-1)^{\frac{p-1}{2}}p\,(p \text{ primer senar}), \qquad -4,\ -8,\ 8.$$

Sigui, doncs, la descomposició de M següent:

$$M = M_1 \dots M_r, \qquad M_i \text{ discriminant primer}, \qquad i = 1, \dots, r.$$

Posem $\Gamma := \{\gamma = (\gamma(1)\dots\gamma(r)) \in \mathbb{Z}^r;\ \gamma(i) \in \{0, 1\},\ \text{per a } i = 1, \dots, r\}$ i per a $\gamma \in \Gamma$, sigui:

$$M_\gamma := M_1^{\gamma(1)} \dots M_r^{\gamma(r)}.$$

M_γ s'anomena divisor discriminantal de M i a l'extensió quadràtica $K(\sqrt{M_\gamma})|K$ l'anomenarem extensió discriminantal de K.

Vegem-ne algunes propietats:

Donat $\gamma \in \Gamma$, sigui $\bar{\gamma} \in \Gamma$ tal que:

$$\bar{\gamma}(i) = 1 - \gamma(i), \text{ per a tot } i = 1, \dots, r$$

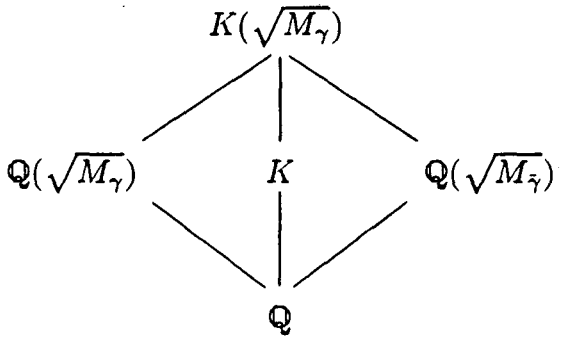
aleshores:

LEMA 3.3.

(a) *$K(\sqrt{M_\gamma})|K$ és no-ramificada als primers finits de K.*
(b) *$K(\sqrt{M_\gamma}) = K(\sqrt{M_{\gamma'}})$ sii $\gamma' = \gamma$ o $\gamma' = \bar{\gamma}$.*
(c) *Sigui $L|K$ una extensió quadràtica no-ramificada als primers finits de K. Aleshores $L = K(\sqrt{M_\gamma})$, per algun $\gamma \in \Gamma$.*

DEMOSTRACIÓ:

Per a provar (a) considerem el diagrama següent:



$\mathcal{D}(\mathbb{Q}(\sqrt{M_\gamma})|\mathbb{Q}) = M_\gamma$, $\mathcal{D}(\mathbb{Q}(\sqrt{M_{\bar{\gamma}}})|\mathbb{Q}) = M_{\bar{\gamma}}$ i $(M_\gamma, M_{\bar{\gamma}}) = 1$, per tant,

$$\mathcal{D}(K(\sqrt{M_\gamma})|\mathbb{Q}) = M_\gamma^2 \cdot M_{\bar{\gamma}}^2 = M^2.$$

Finalment, de :

$$\mathcal{D}(K(\sqrt{M_\gamma})|\mathbb{Q}) = N_{K|\mathbb{Q}}(\mathcal{D}(K(\sqrt{M_\gamma})|K))(\mathcal{D}(K|\mathbb{Q}))^2$$

obtenim

$$N_{K|\mathbb{Q}}(\mathcal{D}(K(\sqrt{M_\gamma})|K)) = 1.$$

Suposem, ara, per a provar (b), que:

$$K(\sqrt{M_\gamma}) = K(\sqrt{M_{\gamma'}}) \Longleftrightarrow M_\gamma M_{\gamma'} \in K^{*^2}.$$

De fet, hem de tenir $M_\gamma M_{\gamma'} \in \mathcal{O}_K^2$. Però de:

$$M_\gamma M_{\gamma'} = \left(\frac{x + y\sqrt{M}}{2}\right)^2, \qquad x, y \in \mathbb{Z},$$

obtenim

$$4M_\gamma M_{\gamma'} = x^2 + y^2 M + 2xy\sqrt{M}.$$

Per tant, $xy = 0$. Si $y = 0$, aleshores $\gamma' = \gamma$. Si $x = 0$, és el cas de $\gamma' = \bar{\gamma}$.

La propietat (b) ens permet, doncs, comptar el nombre d'extensions discriminantals de K. Vegem que aquest nombre és justament 2^{s-1}, on s és el nombre de primers que ramifiquen a K o, equivalentment, el nombre de factors primers de M.

En efecte, considerem la descomposició de M en discriminants primers:

$$M = M_1 \ldots M_r.$$

Observem que, en qualsevol cas ($M \equiv 1 \pmod 4$, $M \not\equiv 1 \pmod 4$), tenim $r = s$. Així, el nombre de divisors discriminantals de M és 2^s i identificant -per la propietat (b)- dos a dos els divisors discriminantals obtenim el nombre d'extensions discriminantals.

Per altra part, per la teoria de cossos de classes sabem que el nombre d'extensions quadràtiques no-ramificades en els primers finits de K és, precisament, el nombre de subgrups d'índex dos (i u) del grup de classes d'ideals estricte H_K^+ i aquest és:

$$[H_K^+ : H_K^{+^2}] = 2^{s-1},$$

aquesta darrera igualtat per la teoria de gèneres de cossos quadràtics. Això prova (c) ∎

REMARQUES 3.3.2:

(i) Per una altra demostració de l'apartat (c) del lema 3.3, vegi's [Go-Lu].

(ii) Obsevem que en la prova de l'apartat (c) del lema s'està comptant el nombre de corbes el·líptiques sobre K amb invariant j fixat i bona reducció arreu. És a dir, si $j \in J$, aleshores:

$$\#(Ell(j) \cap Ell_\phi) = 2^{s-1},$$

on s és el nombre de factors primers de M.

Considerem $c \in H_K^+$ tal que $c^\sigma = c$. Una tal classe s'anomena ambigua estricta i ve també caracteritzada per: $c^2 = 1$. Per extensió, anomenarem a $c \in H_K$ ambigua si satisfà: $c^2 = 1$ (a H_K^+).

Siguin $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ els divisors primers de M; aleshores el nombre de classes ambigües estrictes és 2^{s-1} i cada classe conté exactament dos divisors del tipus:

$$\mathfrak{p}_{i_1} \ldots \mathfrak{p}_{i_k}, \qquad 1 \leq i_1 < \cdots < i_k \leq s \, (k = 0, 1, \ldots, s).$$

DEFINICIÓ: Direm que una classe $c \in H_K$ ambigua és senar si $c = \text{classe}\,(\mathfrak{p}_{i_1} \ldots \mathfrak{p}_{i_k})$ amb $(N(\mathfrak{p}_{i_1} \ldots \mathfrak{p}_{i_k}), 2) = 1$. En altre cas, direm que la classe és parell.

TEOREMA 3.4.

Sigui $E|K$ una corba el·líptica semistable. Existeix un torcement seu semistable i amb model minimal global si i sols si $a(E|K)$ és ambigua senar.

DEMOSTRACIÓ:

Suposem χ un caràcter quadràtic tal que E^χ té reducció semistable i model minimal global. Aleshores, χ és no-ramificat als primers finits i de la relació (3.14) es té:

$$1 = a(E|K)a(\chi). \tag{3.15}$$

Però, pel lema 3.3, χ correspon a una extensió discriminantal de $K : K(\sqrt{M_\gamma})$, $\gamma \in \Gamma$. Fent abús de notació escriurem $a(M_\gamma) := a(\chi)$.

Explicitem $a(M_\gamma)$. Per això, siguin $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ els diferents divisors primers de M, ordenats de manera que:

$$\mathfrak{p}_i | p_i, \qquad i = 1, \ldots, s, \qquad p_1 < p_2 < \cdots < p_s.$$

Sigui $M = M_1 \ldots M_s$ la descomposició de M en producte de discriminants primers tal que $\mathfrak{p}_i | M_i$, $i = 1, \ldots, s$. Llavors, de $a(M_\gamma) = \text{classe } \left(\sum \frac{1}{2} v(M_\gamma) \cdot v \right)$ obtenim:

$$a(M_\gamma) = \begin{cases} \text{classe } (\mathfrak{p}_2^{\gamma(2)} \ldots \mathfrak{p}_s^{\gamma(s)}) & \text{si } m \equiv 3 \pmod 4 \\ \text{classe } (\mathfrak{p}_1^{\gamma(1)} \ldots \mathfrak{p}_s^{\gamma(s)}) & \text{en altre cas.} \end{cases} \tag{3.16}$$

Per tant, $a(M_\gamma)$ és, en qualsevol cas, una classe ambigua senar (notem que quan $m \equiv 2 \pmod 4$: classe $(\mathfrak{p}_1) =$ classe $(\mathfrak{p}_2 \ldots \mathfrak{p}_s)$).

De (3.15) tenim:

$$a(E|K) = a(M_\gamma).$$

Això prova la necessitat de les condicions.

La suficiència és clara, ja que de (3.16) es desprèn que $(a(M_\gamma))_{\gamma \in \Gamma}$ cobreixen totes les classes ambigües senars de H_K ∎

COROL·LARI 3.4.1.

Sigui K amb ε tal que $tr(\varepsilon) \equiv 0$ (mod 4) si $m \equiv 3$ (mod 4). Aleshores, si $E|K$ és una corba el·líptica semistable existeix un torcement seu semistable i amb model minimal global si i sols si $a(E|K)$ és ambigua.

DEMOSTRACIÓ:

En efecte, si $m \not\equiv 3 \pmod 4$ tota classe ambigua és ja senar.

Quan $m \equiv 3 \pmod 4$ siguin $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ els divisors primers de M, amb $\mathfrak{p}_1 | 2$.

De $N(\varepsilon) = 1$, tenim:

$$(1 + \varepsilon)^\sigma = \varepsilon^\sigma (1 + \varepsilon).$$

Per tant, $(1+\varepsilon)\mathcal{O}_K = (a) \cdot \mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_s^{\alpha_s}$, a, $\alpha_i \in \mathbb{N}$ $(i = 1, \ldots, s)$. Però de $N(1+\varepsilon) = 2 + tr(\varepsilon) \equiv 2 \pmod 4$, hem de tenir $\alpha_1 = 1$. Així, classe $(\mathfrak{p}_1) =$ classe $(\mathfrak{p}_2^{\alpha_2} \ldots \mathfrak{p}_s^{\alpha_s})$ ∎

REMARQUES 3.3.3:

(i) Utilitzant les mateixes notacions que en la demostració del corol·lari anterior, remarquem que quan $m \equiv 3 \pmod 4$ i $tr(\varepsilon) \equiv 2 \pmod 4$ aleshores:

$$\text{classe } (\mathfrak{p}_1) \neq \text{ classe } (\mathfrak{p}_2^{\alpha_1} \ldots \mathfrak{p}_s^{\alpha_s}) \text{ per a tot } \alpha_i \in \mathbb{N} \qquad (i = 1, \ldots, s).$$

En efecte, això és equivalent a veure que tota classe ambigua principal és senar. Però les úniques relacions a H_K entre classe $(\mathfrak{p}_1), \ldots,$ classe $(\mathfrak{p}_s)$ vénen donades

per: $\sqrt{m}$, si $m < 0$ i $\sqrt{m}$, $1+\varepsilon$, si $m > 0$ ([cf. Ha, cap. 29]). Només cal veure, ara, que 2 divideix $N(1+\varepsilon)$ amb exponent parell. De $tr(\varepsilon) \equiv 2 \pmod 4$ posem $\varepsilon = x + y\sqrt{m}$, amb $x = -1 + 2^\alpha a$, $\alpha, a \in \mathbb{N}$, $(a,2) = 1$, $\alpha \geq 1$. Finalment, de $x^2 - y^2 m = 1$ tenim la relació: $2^{\alpha+1}(2^{\alpha-1}a^2 - a) = y^2 m$, d'on deduïm que $\alpha \equiv 1 \pmod 2$ i de $N(1+\varepsilon) = 2(1+x)$ s'obté el resultat.

(ii) Comptem corbes el·líptiques sobre K amb b.r.a. i model minimal global. Per això, denotem per:

$$Ell(j)_g = \{E|K;\, j(E) = j \text{ i } a(E|K) = 1\}.$$

Siguin $j \in J$ i $d \in K^*/K^{*2}$ tals que E_j^d té bona reducció arreu. Pel teorema 3.4, $Ell(j)_g \cap Ell_\phi \neq \phi$ sii $a(E_j^d)$ és ambigua senar. En aquestes hipòtesis es té:

$$\#(Ell(j)_g \cap Ell_\phi) = \begin{cases} 1 & \text{si } N(\varepsilon) = -1 \\ 2 & \text{si } N(\varepsilon) = 1 \text{ i } tr(\varepsilon) \equiv 0 \pmod 4 \text{ quan } m \equiv 3 \pmod 4 \\ 4 & \text{si } m \equiv 3 \pmod 4,\ tr(\varepsilon) \equiv 2 \pmod 4. \end{cases}$$

Estem suposant sempre $m > 0$, ja que en el cas imaginari Stroeker [Stro] demostrà que $\mathrm{Ell}(j)_g \cap \mathrm{Ell}_\phi = \phi$. Vegi's també l'exemple 4, més endavant.

En efecte, per (3.15), es tracta de comptar totes les extensions discriminantals $K(\sqrt{m_\gamma})$, $\gamma \in \Gamma$, satisfent: $a(M_\gamma) = 1$. Si $N(\varepsilon) = -1$, l'única relació entre classe $(\mathfrak{p}_1), \ldots,$ classe $(\mathfrak{p}_s)$ ve donada per $\sqrt{m}$. Si $N(\varepsilon) = 1$, les úniques relacions vénen donades per $\sqrt{m}$, $1+\varepsilon$. Si $tr(\varepsilon) \equiv 0 \pmod 4$ quan $m \equiv 3 \pmod 4$, per (3.16), només ens quedem amb la relació senar $\sqrt{m}$. Finalment, observem que a cadascuna d'aquestes relacions li correspon una única extensió discriminantal si $m \not\equiv 3 \pmod 4$ i exactament dues extensions si $m \equiv 3 \pmod 4$, ja que en aquest cas es té per $4 \nmid M_\gamma : a(M_\gamma) = a(-4M_\gamma)$.

COROL·LARI 3.4.2.

Sigui K amb $N(\varepsilon) = -1$, $(h_K, 3) = 1$ i el 4-rang de H_K zero. Aleshores, tota corba el·líptica $E|K$ amb b.r.a. admet un torcement amb b.r.a. i model minimal global.

DEMOSTRACIÓ:

De $a(E|K)^{12} = 1$ tenim $a(E|K)^2 = 1$ i apliquem el corol·lari 3.4.1 ∎

EXEMPLE 4.

Suposem $m < 0$ i sigui $E|K$ amb bona reducció arreu, $a(E|K)^2 = 1$ i $j(E) \in \mathbb{Z}$. Aleshores $a(E|K)$ és parell.

DEMOSTRACIÓ:

Com que $j(E) \in \mathbb{Z}$, deduïm de les condicions de Setzer (exemple 3) els següents fets:

1) $m = \pm D$.

En efecte, de $a(E|K)^2 = 1$ tenim $\pm\Delta_F \in K^{*^2}$, per a qualsevol model de Weierstraß F de E i, per tant, de $j - 1728 = \dfrac{c_6^2(F)}{\Delta_F}$ obtenim $\pm D \in K^{*^2}$.

2) $(D, 2) = 1$.

En efecte, si $2|D$ per a (iii) es té $D \equiv m + 4 \pmod 8$ i, així, $D = -m$. Això es contradiu amb b (iii), ja que $-D < 0$, no és una norma a K!.

3) $m \equiv -1 \pmod 8$.

En efecte, de b (ii) i b (i): $\delta D > 0$ i $m = -\delta D$, amb $\delta D \equiv 1 \pmod 8$.

Considerem la corba el·líptica E_j. Provarem que si $d = \dfrac{2j}{\sqrt{-|j - 1728|}}$ llavors $E_j^{\pm d}$ té b.r.a.

En efecte, de $\Delta(E_j) = \dfrac{6^{12} j^2}{(j - 1728)^3}$ tenim que $d \equiv d_v \pmod 2$ per a tot $v \in \Sigma$ i de $2\sqrt{m} \equiv (1 + \sqrt{m})^2 \pmod 8$, tenim:

$$\pm d/f(r) \equiv \alpha^2 \pmod 8, \qquad \alpha \in K$$

on prenem

$$f(r) = \begin{cases} -1 & \text{si } v(j) = 0 \\ \dfrac{-24j}{j - 1728} & \text{si } v(j) > 0. \end{cases}$$

Finalment, de $\Delta(E_j^{\pm d}) = \dfrac{6^{12} 2^6 j^8}{(j - 1728)^6}$ tenim que $2^l \| \Delta(E_j^{\pm d})$ on $l \equiv 6 \pmod{12}$ i d'aquí, per la remarca 3.3.3 (i), $a(E_j^{\pm d}|K)$ és parell ∎

REMARCA:

Krämer, de fet, a [Krä] demostrà el següent resultat: Si E és una corba el·líptica sobre un cos quadràtic imaginari amb b.r.a. i $a(E|K)^4 = 1$ aleshores hem de tenir $j(E) \in \mathbf{Z}$. Així, aquest resultat juntament amb l'obtingut a l'exemple 4 impliquen el teorema de Stroeker [Stro] que afirma que sobre cossos quadràtics imaginaris no hi han corbes el·líptiques amb b.r.a. i model minimal global.

BIBLIOGRAFIA

[Ar] E. Artin, "Collected works," Addison-Wesley, Reading, Mass., pp. 229–231.

[Ba-La] P. Bayer i J.-C. Lario, *On Galois representations defined by torsion points of modular elliptic curves*, preprint.

[Bo-Sha] Z.I. Borevich i I.R. Shafarevich, "Number Theory," Academic Press, 1966.

[Co1] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. **144(2)** (1990), 237–258.

[Co2] ———, *Courbes elliptiques à bonne réduction d'invariant j fixé*, C.R. Acad. Sci. Paris **t. 311, Série I** (1990), 667–670.

[El-Gru-Me] J. Elstrod, F. Grunewald i J. Mennicke, *On the group* $PSL(2,\mathbb{Z}[i])$, Proc. conf. Journées Aritmétiques 1980, LMS 56, 1982, 255–283.

[Fre] G. Frey, *Links between solutions of* $A - B = C$ *and elliptic curves*, Number theory. Ulm 1987, Lecture Notes in Mathematics **1380**, Springer-Verlag, 1987.

[Frö] A. Fröhlich, *Discriminants of relative extensions and the existence of integral bases*, Mathematika **7** (1960), 15–22.

[Go-Lu] S.K. Gogia i I.S. Luthar, *Quadratic unramified extensions of* $\mathbb{Q}(\sqrt{d})$, J. Reine Angew. Math. **298** (1978), 108–111.

[Ha] H. Hasse, "Number theory," Grundlehren der mathematischen Wissenschaften **229**, Springer-Verlag, 1980.

[Hu] D. Husemöller, "Elliptic curves," Graduate Texts in Mathematics **111**, Springer-Verlag, 1986.

[Ja-La] H. Jacquet i R. Langlands, "Automorphic forms on $GL(2)$," Lecture Notes in Mathematics **114**, Springer-Verlag, 1970.

[Kra] A. Kraus, *Quelques remarques à propos des invariants* c_4, c_6 *et* Δ *d'une courbe elliptique*, Acta Arithmetica **54** (1989), 75–80.

[Krä] N. Krämer, *Beiträge zur Arithmetik imaginärquadratischer Zahlkörper*, Tesi doctoral, Universität Bonn, 1984.

[Las] M. Laska, *Elliptic curves over number fields with prescribed reduction type*, Aspects of Math. **4**, Friedr. Vieweg & Sohn, Braunschweig/Wiesbaden, 1983.

[Nar] W. Narkiewicz, "Elementary and analytic theory of algebraic numbers," Monographie Matematyczne **57**, PWN-Polish scientific Publishers, Warszawa, 1974.

[Né] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, IHES Publ. Math. **21** (1964), 361–482.

[Neuk] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59–116.

[Neum] O. Neumann, *Zur Reduktion der elliptischen Kurven*, Math. Nachr. **46** (1970), 285–310.

[Og1] A.P. Ogg, *Abelian curves of 2-power conductor*, Proc. Camb. Philos. Soc. **62** (1966), 143–148.

[Og2] ———, *Abelian curves of small conductor*, J. Reine Angew. Math. **226** (1967), 204–215.

[Og3] ———, *Elliptic curves and wild ramification*, Am. J. of Math. **89** (1967), 1–21.

[Pi] R.G.E. Pinch, *Elliptic curves with good reduction away from 2*, Proc. Camb. Philos. Soc. **96** (1984), 25–38.

[Se] J.-P. Serre, "Corps locaux," Publications de l'Institut de Mathématique de l'Université de Nancago **VIII**, Hermann, Paris, 1962.

[Se-Ta] J.-P. Serre i J. Tate, *Good reduction of abelian varieties*, Annals of Math. **88** (1968), 492–517.

[Set1] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math. **74(1)** (1978), 235–250.

[Set2] ———, *Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant*, Illinois J. Math. **25(2)** (1981), 233–245.

[Sil1] J.H. Silverman, *Weierstrass equations and the minimal discriminant of an elliptic curve*, Mathematika **31** (1984), 245–251.

[Sil2] ———, "The Arithmetic of Elliptic Curves," Graduate Texts in Mathematics **106**, Springer-Verlag, 1986.

[Ste] G. Stevens, Carta a l'autor.

[STN] Seminari de Teoria de Nombres de Barcelona, 1986-87, apunts (n.e.).

[Stro] R.J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*, Pacific J. Math. **108(2)** (1983), 451–463.

[Ta1] J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

[Ta2] ———, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable IV, Lecture Notes in Math. **476**, Springer-Verlag, 1975, pp. 33–52.

[We] A. Weil, "Dirichlet series and Automorphic forms," Lecture Notes in Mathematics **189**, Springer-Verlag, 1971.