Riv. Mat. Univ. Parma 8 (1957), 81-92

MARCO CUGIANI (*)

Forme cubiche nei domini P-adici.

I. – Introduzione.

In un precedente lavoro (1) abbiamo affrontato il problema di determinare le condizioni sotto le quali un intero P-adico β è rappresentabile mediante una forma del tipo $x^2 - \alpha y^2$, con α intero P-adico fisso, ed x, y variabili nel dominio P-adico di integrità D_P.

Quella ricerca si richiamava e presentava molti punti di contatto con i classici studi di K. HENSEL sulle forme quadratiche nei corpi P-adici (2).

Noi vogliamo adesso mostrare come il tipo di ragionamento seguito nel lavoro richiamato si possa immediatamente adattare per ottenere analoghi risultati a proposito delle forme cubiche. Più precisamente ci ripromettiamo di stabilire sotto quali condizioni un intero P-adico β è rappresentabile con una forma del tipo $x^3 - \alpha y^3$, o, se vogliamo, sotto quali condizioni è solubile, in interi P-adici x, y, l'equazione

$$x^3 - \alpha y^3 = \beta \tag{a}$$

con α e β interi P-adici.

Per amore di brevità abbiamo trattato completamente solo il caso $P \neq 3$, limitandoci per il caso $P = 3$ ad esporre i risultati, di cui ometteremo la dimostrazione. Essa del resto non sarebbe difficile e può esser condotta sulla base

---

(*) Indirizzo: Istituto Matematico F. ENRIQUES, Università, Via C. Saldini 50, Milano, Italia.

(1) M. CUGIANI, *Approssimazioni quadratiche nei domini P-adici*, Ann. Mat. Pura Appl. (4) **44** (1957), 1-22.

(2) Su tale questione si veda anche: B. W. JONES, **The arithmetic theory of quadratic forms**, (Carus mathematical Monographs, N. 10) J. Wiley and Sons, New York 1950 (cfr. §§ 8, 26).

di procedimenti del tutto analoghi a quelli da noi sempre seguiti in questo tipo di ricerche.

Passiamo in primo luogo ad esporre i risultati della presente ricerca; qui e nel seguito ci serviremo di notazioni e terminologia già impiegate ed illustrate nel precedente lavoro.

È quasi superfluo osservare che alla equazione (a) si può indifferentemente sostituire la seguente:

(b) $$x^3 + \alpha y^3 = \beta,$$

solubile od insolubile insieme alla (a).

Teorema A. *Sia* $P \neq 3$ *e siano*

$$\alpha = \sum_{i=r}^{\infty} a_i P^i, \qquad \beta = \sum_{i=s}^{\infty} b_i P^i$$

interi P-adici fissati ($r = \operatorname{ord} \alpha$, $s = \operatorname{ord} \beta$);

condizione necessaria e sufficiente perchè sia solubile, in interi P-adici x, y, *l'equazione*

$$x^3 + \alpha y^3 = \beta,$$

è che sia verificata una delle seguenti circostanze:

1°) *sia* β *un* D_P*-cubo* (*caso ovvio*);

2°) *non sia* β *un* D_P*-cubo, e sia invece* α *un* D_P*-cubo*; *risulti inoltre*

per $P \neq 7$, $r \leqslant s$; *per* $P = 7$, $r < s$ *oppure* $r = s$, *ma in quest'ultimo caso si abbia in più* $b_s = 2, 5$;

3°) *nè* β *nè* α *sia un* D_P*-cubo, ma si abbia*

$$r \leqslant s \qquad ed \qquad r \equiv s \pmod 3,$$

nel caso poi che sia $r \equiv s \not\equiv 0 \pmod 3$ *risulti inoltre il prodotto* $a_r^{-1} \cdot b_s$ *un residuo cubico* (mod P).

Da questo Teorema si deduce immediatamente, in analogia con il caso delle forme quadratiche [3], il seguente

---

[3] Loc. cit. in [1], Teorema C, pag. 4.

Corollario A. *Sia* $P \neq 3, 7$. *Condizione necessaria e sufficiente perchè tutti i numeri di* D_p *siano rappresentabili colla forma* $x^3 + \alpha y^3$ *è che sia* α *contemporaneamente un* D_p*-cubo e una unità di* D_p.

Ne consegue, e anche qui la cosa è immediata, che, in base alla caratterizzazione dei D_p-cubi come verrà stabilita al Lemma B del n. successivo, vale il seguente

Corollario B. *I numeri* α, *tali che la forma* $x^3 + \alpha y^3$ *risulti atta a rappresentare tutti i numeri di* D_p, *costituiscono un insieme* J *per cui vale una delle relazioni*:

$$\text{mes } J = (P-1)/P \qquad \textit{se} \qquad P \equiv 2 \pmod 3,$$

$$\text{mes } J = (P-1)/(3P) \qquad \textit{se} \qquad P \equiv 1 \pmod 3,\ P > 7;$$

nel caso $P = 7$ *l'insieme* J *è vuoto e si ha pertanto* mes $J = 0$.

Qui con mes J si indica al solito la misura di Haar scelta in modo che risulti mes $D_p = 1$.

Per quanto si riferisce al caso $P = 3$ ci limiteremo ad enunciare il seguente

Teorema B. *Siano* α *e* β *interi 3-adici che rappresenteremo nella forma*

$$\alpha = \sum_{i=r}^{\infty} A^{(i)} \cdot 27^i, \qquad \beta = \sum_{i=s}^{\infty} B^{(i)} \cdot 27^i$$

$(0 < A^{(r)} < 27,\ 0 < B^{(s)} < 27;\ 0 \leqslant A^{(i)} < 27,\ 0 \leqslant B^{(i)} < 27)$. *Condizione sufficiente e necessaria perchè la* (b) *sia solubile in* D_3 *è che sia verificata una delle seguenti circostanze*:

1°) *sia* $r > s$ *e* β *un* D_3*-cubo* [*cioè* $B^{(s)} \equiv 1, 8 \pmod 9$];

2°) *sia* $r = s$, α *un* D_3*-cubo* [*cioè* $A^{(r)} \equiv 1, 8 \pmod 9$] *ed inoltre* $B^{(s)}$ *soddisfi ad una delle relazioni*

$$B^{(s)} \equiv 0, 1, 2, 7, 8 \pmod 9;$$

3°) *sia* $r < s$ *ed* α *un* D_3*-cubo*;

4°) *sia* $r \leqslant s$ *ed inoltre si presenti uno dei seguenti accoppiamenti*:

$A^{(r)} \equiv 2,\ 7 \pmod 9$, $\quad B^{(s)} \equiv 1, 2, 3, 6, 7, 8 \pmod 9$;

$A^{(r)} \equiv 4,\ 5 \pmod 9$, $\quad B^{(s)} \equiv 1, 3, 4, 5, 6, 8 \pmod 9$;

$A^{(r)} \equiv 3,\ 6 \pmod 9$, $\quad B^{(s)} \equiv 1, 2, 4, 5, 7, 8 \pmod 9$ *oppure* $B^{(s)} \equiv \pm A^{(r)} \pmod{27}$;

$A^{(r)} \equiv 0 \pmod 9$, $\quad B^{(s)} \equiv 0, 1, 8 \pmod 9$.

Da questo Teorema discende immediatamente, in perfetta analogia con quanto si è visto per le forme quadratiche (4) nel caso $P = 2$, il seguente

Corollario C. *In* D_3 *non esiste alcun numero* α *tale che la forma* $x^3 + \alpha y^3$ *sia atta a rappresentare tutti gli elementi del dominio.*

La stessa affermazione vale, per quanto si è detto sopra, per il dominio D_7. I domini D_3 e D_7 hanno dunque un comportamento eccezionale; per tutti gli altri D_p vale infatti il Corollario A. Si può rilevare qui una differenza dal caso delle forme quadratiche dove avevamo incontrato un solo dominio, il D_2, che presentasse un analogo comportamento eccezionale.

II. – Lemmi preliminari.

Lemma *A*. *Sia* P *un numero primo* $\neq 7$, *e siano* m *ed* n *interi, non divisibili per* P, *allora è sempre solubile la congruenza*

$$x^3 + m y^3 \equiv n \pmod P$$

in interi x, y *di cui sia almeno* $y \not\equiv 0 \pmod P$.

Per $P = 3$ il Lemma è immediatamente verificabile, così pure nel caso che sia $P \equiv 2 \pmod 3$, poichè allora tutti gli interi sono residui cubici di P e basta porre, ad esempio, $x = 0$, $y^3 = n \cdot m^{-1}$.

Se $P \equiv 1 \pmod 3$ ed è $P \geqslant 19$ la nostra affermazione discende immediatamente da un teorema di Hurwitz (5), secondo il quale la congruenza [$abc \not\equiv 0 \pmod P$]

$$ax^3 + by^3 + cy^3 \equiv 0 \pmod P$$

(4) Loc. cit. in (1), teorema F, pag. 6.

(5) Il teorema, di cui la proposizione qui invocata è un caso particolare, si trova in: A. Hurwitz, *Über die Kongruenz* $ax^e + by^e + cz^e \equiv 0 \pmod p$, J. Math. **136** (1909), 272-292. Tale teorema è riportato anche in P. Bachmann, **Das Fermatproblem**, W. de Gruyter & Co., Berlin 1919 (cfr. pp. 86-95).

è solubile in interi x, y, z, non divisibili per P se è positiva l'espressione $P + 1 - 2\sqrt{P} - 3\eta$, dove $\eta \leqslant 3$.

Si verifica poi direttamente che la proposizione è vera per $P = 13$, e il nostro Lemma è così dimostrato.

Osservazione 1ª. Nel caso $P = 7$ il Lemma A non vale in generale, come si vede subito osservando che ad esempio è insolubile la congruenza

$$x^3 + y^3 \equiv 3 \pmod 7.$$

In particolare se m è un residuo cubico il Lemma A vale solo se $n \equiv 2, 5$; ed è poi sempre valido se m ed n non sono residui cubici (mod 7), come è facile verificare direttamente.

Passiamo adesso al

Lemma B. *Condizione necessaria e sufficiente perchè l'intero P-adico*

$$m = \sum_{i=s}^{\infty} m_i P^i \qquad (\text{con } m_s \neq 0)$$

sia un D_r-cubo, è che risulti in ogni caso

$$s \equiv 0 \pmod 3$$

ed inoltre:

per $P \neq 3$ sia m_s un residuo cubico (mod P);

per $P = 3$ sia $m_s = 1$, $m_{s+1} = 0$, oppure $m_s = m_{s+1} = 2$.

La dimostrazione è perfettamente analoga a quelle dei corrispondenti lemmi 1° e 2° esposte in loc. cit. in (1), e pertanto verrà qui schizzata brevemente (6).

Sia dapprima $P \neq 3$.

La condizione è ovviamente necessaria poichè se è $x^3 = m$, con $x = \sum_{i=r}^{\infty} x_i P^i$, sarà $m = x_i^3 P^{3i} + H \cdot P^{3i+1}$, H intero P-adico ed $x_i^3 \equiv m_s \pmod P$, $s = 3i$.

(6) È chiaro che questo Lemma potrebbe essere dedotto dai classici risultati esposti in: K. HENSEL, **Zahlentheorie**, Göschen, Berlin und Leipzig 1913 (cfr. pag. 234 e seguenti). Abbiamo preferito, come in altri casi, darne una dimostrazione fondata su quei concetti del tutto elementari a cui abbiamo uniformati questi lavori.

Per dimostrarne la sufficienza partiamo dalla osservazione che se i, n, X_i soddisfano alle condizioni

$$0 < X_i < P^{i+1}, \qquad i = n - 2 \cdot \operatorname{ord} X_i, \qquad X_i^3 \equiv M_n \pmod{P^{n+1}}$$

(qui al solito abbiamo posto $M_n = \sum_{i=s}^{n} m_i P^i$), allora si potrà determinare univocamente x_{i+1} in modo che

$$X_{i+1}^3 = (X_i + x_{i+1} P^{i+1})^3 \equiv M_n + m_{n+1} P^{n+1} \pmod{P^{n+2}},$$

come si verifica con le solite considerazioni.

Supposto ora $s = 3r$, essendo m_s un residuo cubico (mod P), scegliamo x_r $(0 < x_r < P)$ in guisa che sia $x_r^3 \equiv m_s \pmod P$, onde posto $X_r = x_r P^r$, essendo $M_s = m_s P^s$ ed $X_r^3 \equiv M_s \pmod{P^{s+1}}$, per l'osservazione precedente, grazie al solito processo di induzione, il nostro Lemma è dimostrato per $P \neq 3$.

Analogamente si procede per $P = 3$.

La condizione è ovviamente necessaria, poichè da $x^3 = m$ si deduce $m = x_i^3 \cdot 3^{3i} + x_i^2 x_{i+1} \cdot 3^{3i+2} + H \cdot 3^{3i+3}$ con H intero 3-adico ed $s = 3i$, e si ha quindi, per $m_s = 1$ che è $x_i = 1$ e perciò $m_{s+1} = 0$; per $m_s = 2$ è $x_i = 2$ e perciò $m_{s+1} = 2$.

Per dimostrarne la sufficienza partiamo dall'osservazione, analoga alla precedente, che se i, n, X_i soddisfano alle condizioni

$$0 < X_i < 3^{i+1}, \qquad i = n - 1 - 2 \cdot \operatorname{ord} X_i \qquad X_i^3 \equiv M_n \pmod{3^{n+1}},$$

allora si potrà determinare, univocamente, x_{i+1} in modo che risulti

$$X_{i+1}^3 = (X_i + x_{i+1} 3^{i+1})^3 \equiv M_n + m_{n+1} \cdot 3^{3i+1} \pmod{3^{n+2}},$$

come si può, con ovvi calcoli, immediatamente verificare.

Se ora $s = 3r$, posto $x_r = m_s$, sarà $x_r^3 \equiv m_s \pmod 3$ e si potrà scegliere (essendo per ipotesi $m_{s+1} = 0$, per $m_s = 1$, ed $m_{s+1} = 2$, per $m_s = 2$) x_{r+1} in guisa che risulti:

$$X_{r+1}^3 = (x_r \cdot 3^r + x_{r+1} \cdot 3^{r+1})^3 \equiv M_{s+2} = m_s \cdot 3^s + m_{s+1} \cdot 3^{s+1} + m_{s+2} \cdot 3^{s+2} \pmod{3^{s+3}};$$

basterà a tal fine che sia $x_{r+1} = m_{s+2}$.

Ora, in base alla precedente osservazione, per il solito processo d'induzione il nostro Lemma è completamente dimostrato.

Osservazione 2ª. Se $P \equiv 2 \pmod 3$ allora tutti i resti (mod P) sono residui cubici di P. Quindi nel caso $P \equiv 2 \pmod 3$ si può affermare che sono D_p-cubi tutti i numeri m tali che risulti ord $m \equiv 0 \pmod 3$.

Ne segue che in un dominio D_p con $P \equiv 2 \pmod 3$ la misura dell'insieme dei D_p-cubi è data da

$$\frac{P-1}{P} + \frac{P-1}{P^4} + \frac{P-1}{P^7} + \ldots = \frac{P-1}{P}\,\frac{P^3}{P^3-1} = \frac{P^2}{P^2+P+1}\,.$$

Invece in un dominio D_p con $P \equiv 1 \pmod 3$ la misura dell'insieme dei D_p-cubi è data da

$$\frac{P-1}{3P} + \frac{P-1}{3P^4} + \ldots = \frac{1}{3}\,\frac{P^2}{P^2+P+1}\,.$$

Infine in D_3 la misura dei D_3-cubi è data da

$$\frac{2}{9} + \frac{2}{9\cdot 3^3} + \frac{2}{9\cdot 3^6} + \ldots = \frac{2}{9}\cdot\frac{1}{1-(1/27)} = \frac{2}{9}\cdot\frac{27}{26} = \frac{3}{13}\,.$$

Per contro va notato che, com'è ovvio, ogni D_p-cubo, quando $P \equiv 2 \pmod 3$, oppure $P = 3$, possiede una sola radice cubica in D_p, mentre nel caso $P \equiv 1 \pmod 3$ ogni D_p-cubo possiede tre radici cubiche distinte in D_p.

Passiamo ora a dimostrare il

Lemma C. *Sia $P \neq 3$ e, per $n \geqslant r = \operatorname{ord}\alpha$, sia $A_n = \sum_{i=r}^{n} a_i P^i$ (e quindi $0 < A_n < P^{n+1}$); siano poi assegnate due coppie di numeri interi non negativi i, j ; X_i, Y_j soddisfacenti alle condizioni (per un certo n fisso)*

$$i > (n-2)/3, \qquad j = n - \operatorname{ord}\alpha - 2\cdot\operatorname{ord} Y_j, \qquad j > (n-2-\operatorname{ord}\alpha)/3,$$

$$j > (n-1-\operatorname{ord}\alpha-\operatorname{ord} Y_j)/2\,;$$

e, per $B_n = \sum_{i=0}^{n} b_i P^i$, risulti inoltre soddisfatta la congruenza

$$X_i^3 + \alpha Y_j^3 - \beta \equiv X_i^3 + A_n Y_j^3 - B_n \equiv 0 \pmod{P^{n+1}} \tag{1}$$

e finalmente si abbia $0 < Y_j < P^{j+1}$; ed inoltre $X_i = 0$, oppure

$$0 < X_i < P^{i+1}, \qquad i \geqslant n - 2\cdot\operatorname{ord} X_i, \qquad i > (n-1-\operatorname{ord} X_i)/2.$$

Allora sarà solubile in interi X_{i+h}, Y_{j+h} *anche ogni congruenza del tipo* (h *intero* > 0)

$$X_{i+h}^3 + \alpha Y_{j+h}^3 - \beta \equiv 0 \pmod{P^{n+h+1}}.$$

Basterà far vedere che dalle ipotesi si deduce la solubilità in interi x_{i+1}, y_{j+1} della congruenza

$$(2) \qquad (X_i + x_{i+1} \cdot P^{i+1})^3 + A_{n+1}(Y_j + y_{j+1} \cdot P^{j+1})^3 - B_{n+1} \equiv 0 \pmod{P^{n+2}},$$

mostrando inoltre che le due nuove coppie

$$(3) \qquad i+1, \quad j+1; \qquad X_{i+1} = X_i + x_{i+1} \cdot P^{i+1}, \quad Y_{j+1} = Y_j + y_{j+1} \cdot P^{j+1}$$

soddisfano ancora alle condizioni poste dianzi.

Il nostro Lemma si deduce allora per induzione.

Stante la profonda analogia che questo Lemma presenta col corrispondente lemma 3° dimostrato in loc. cit. in (1), ci limiteremo anche qui a schizzare la dimostrazione.

In quanto alla affermazione che le coppie (3) soddisfano ancora alle ipotesi del Lemma è cosa che si verifica immediatamente osservando che, nel passaggio da (1) a (2), n viene sostituito da $n+1$, mentre ord A_n = ord α, ord X_i (se $X_i \not\equiv 0$) ed ord Y_j rimangono invariati. Anche se fosse $X_i = 0$, $X_{i+1} \not\equiv 0$ avremmo ord $X_{i+1} = i+1$ e quindi da $i > (n-2)/3$ si deduce $i + 1 > \{ n - 1 - (i+1) \}/2$, $\quad i + 1 > n - 2i - 2$.

Tutto si riduce dunque a dimostrare la solubilità della (2). Essa si può scrivere:

$$(X_i + x_{i+1} \cdot P^{i+1})^3 + (A_n + a_{n+1} \cdot P^{n+1})(Y_j + y_{j+1} \cdot P^{j+1})^3 -$$

$$- B_n - b_{n+1} \cdot P^{n+1} \equiv 0 \pmod{P^{n+2}}$$

che, ponendo

$$X_i^3 + A_n \cdot Y_j^3 - B_n = \varrho P^{n+1}, \qquad 3X_i^2 \cdot P^{i+1} = \mu P^{n+1},$$

$$3A_{n+1} Y_j^2 \cdot P^{j+1} = \nu P^{n+1}, \qquad a_{n+1} Y_j^3 = \sigma$$

(dove risultano, per le ipotesi fatte, ϱ, μ, ν, σ interi e $P \nmid \nu$), si riduce con ovvie semplificazioni, sempre ricordando le ipotesi del Lemma, alla relazione

$$\varrho + \sigma + \mu x_{i+1} + \nu y_{j+1} - b_{n+1} \equiv 0 \pmod{P},$$

certamente solubile poichè è almeno $\nu \not\equiv 0 \pmod{P}$.

III. – Dimostrazione del Teorema A.

Dimostriamo adesso il Teorema A, dividendo la dimostrazione in tre parti in corrispondenza alla suddivisione dell'enunciato.

1°) Se β è un D_P-cubo sarà $\beta = h^3$ per almeno un $h \in D_P$; posto $x = h$, $y = 0$ si ottiene quindi una soluzione della (b) e il Teorema è ovvio in questo caso.

2°) Non sia β un D_P-cubo e sia invece α un D_P-cubo. Sarà $r = \operatorname{ord} \alpha \equiv 0 \pmod 3$ ed a_r un residuo cubico (mod P).

Facciamo vedere in primo luogo che la condizione $|\beta|_P \leqslant |\alpha|_P$ è necessaria in ogni caso per la solubilità della (b) quando β non è un D_P-cubo. Infatti nella ipotesi $|\beta|_P > |\alpha|_P$, ossia se fosse $s = \operatorname{ord} \beta < r = \operatorname{ord} \alpha$, sarebbe insolubile la congruenza

$$x^3 - b_s \cdot P^s \equiv 0 \pmod{P^{s+1}},$$

poichè se fosse $x = h$ una soluzione di tale congruenza dovremmo avere $h^3 \equiv 0 \pmod{P^s}$, ossia, posto $P^u \parallel h$, dovrebbe essere $u \geqslant s/3$.

Ma $u > s/3$ comporterebbe $b_s = 0$ contro l'ipotesi che sia $\operatorname{ord} \beta = s$, mentre $u = s/3$ comporterebbe

$$s \equiv 0 \pmod 3; \quad h = P^{s/3} h_1, \quad P \nmid h_1, \quad h_1^3 \equiv b_s \pmod P$$

e sarebbe b_s un residuo cubico, con $3 \mid s$, e quindi β un D_P-cubo, contro l'ipotesi.

Supponiamo dunque $|\beta|_P \leqslant |\alpha|_P$, esisterà allora un $t \geqslant 0$ per cui sia $s = r + t$

Per $t > 0$ vediamo che la congruenza

$$(x_u \cdot P^u)^3 + a_{3u} \cdot P^{3u}\, y_0^3 \equiv 0 \pmod{P^{3u+1}},$$

dove abbiamo posto $r = 3u$, si riduce a

$$x_u^3 + a_{3u} \cdot y_0^3 \equiv 0 \pmod P,$$

che ammette certamente soluzioni con $P \nmid y_0$.

A causa del Lemma C il Teorema è dunque dimostrato in questo caso.

Per $t = 0$ osserviamo che la congruenza

$$x_u^3 \cdot P^{3u} + a_{3u} \cdot P^{3u}\, y_0^3 - b_{3u} \cdot P^{3u} \equiv 0 \pmod{P^{3u+1}}$$

si riduce a

$$x_u^3 + a_{3u} \cdot y_0^3 - b_{3u} \equiv 0 \pmod{P},$$

che ammette certo soluzioni, per il Lemma A, se $P \neq 7$, mentre se $P = 7$ ammette soluzioni, per la Osservazione 1ª, se e soltanto se $b_{3u} = b_s = 2, 5$. Il Teorema è dunque dimostrato anche in questo caso.

3°) Nella dimostrazione fatta a 2°) abbiamo visto che la (b) non è solubile se $|\beta|_p > |\alpha|_p$ quando β non è un D_p-cubo. Supponiamo dunque anche qui $|\beta|_p \leqslant |\alpha|_p$, cioè $s \geqslant r$.

La congruenza

$$x^3 + A_s \cdot y^3 - b_s \cdot P^s \equiv 0 \pmod{P^{s+1}} \tag{4}$$

si può scrivere, ponendo $r = 3u + h, \quad s = r + t, \ (0 \leqslant h < 3, \quad t \geqslant 0)$,

$$x^3 + P^{3u+h} \cdot (a_r + a_{r+1} \cdot P + \ldots + a_s \cdot P^t)\, y^3 - b_s \cdot P^s \equiv 0 \pmod{P^{s+1}};$$

ponendo $x = P^u \cdot \xi$, essa è equivalente alla

$$\xi^3 + P^h \cdot (a_r + \ldots) y^3 - b_s \cdot P^{h+t} \equiv 0 \pmod{P^{h+t+1}}. \tag{5}$$

Sia dapprima $s \not\equiv r \pmod 3$ e quindi certamente $t > 0$, e poniamo $a_r + a_{r+1} \cdot P + \ldots + a_s \cdot P^t = A_s / P^r = A'$.

La (5) diventa:

$$\xi^3 + P^h \cdot A' y^3 - b_s \cdot P^{h+t} \equiv 0 \pmod{P^{h+t+1}}.$$

Essendo $t \not\equiv 0 \pmod 3$, questa congruenza è sempre insolubile. Infatti se è $h = 0$ essa si riduce alla

$$\xi^3 + A' y^3 - b_s \cdot P^t \equiv 0 \pmod{P^{t+1}},$$

ma essendo A' non residuo la $\xi^3 + A' y^3 \equiv 0 \pmod P$ non ammette soluzioni con $\xi, y \not\equiv 0 \pmod P$, perciò la massima potenza di P che divide $\xi^3 + A' y^3$ è uguale a quella che divide il massimo comun divisore fra ξ^3 e y^3 ed è certamente un cubo, mentre $t \not\equiv 0 \pmod 3$.

Se poi $h > 0$ dovrà essere $P \mid \xi$ e ponendo $\xi = P\sigma$ la (5) diventa

$$P^3 \sigma^3 + A' P^h y^3 - b_s \cdot P^{h+t} \equiv 0 \pmod{P^{h+t+1}}$$

ossia, ponendo $h' = 3 - h$,

$$P^{h'} \cdot \sigma^3 + A' y^3 - b_s \cdot P^t \equiv 0 \pmod{P^{t+1}}. \tag{6}$$

Sia ora $t = 3v + t'$ $(0 < t' < 3)$; poichè i primi due termini sono divisibili per potenze di P i cui esponenti sono certamente diversi, dovrà essere $P^v \mid \sigma$, $P^{v+1} \mid y$. Poniamo allora $\sigma = P^v \cdot \omega$, e la (6) si riduce a

$$P^{h'} \cdot \omega^3 - b_s \cdot P^{t'} \equiv 0 \pmod{P^{t'+1}} \tag{7}$$

la quale è certo insolubile, come è ovvio se $h' \neq t'$, ricordando che $t' + 1 \leqslant 3$ e quindi deve essere $P \nmid \omega$; e come si vede facilmente se $h' = t'$ pensando che in tal caso è

$$h' \equiv t \pmod 3, \qquad h + t \equiv 0 \pmod 3, \qquad s = 3u + h + t \equiv 0 \pmod 3,$$

e quindi b_s non è un residuo cubico poichè per ipotesi β non è un D_P-cubo.

Esaminiamo adesso il caso $s \equiv r \pmod 3$.

Posto $t = 3v$, la (5) diventa

$$\xi^3 + P^h \cdot A' y^3 - b_s \cdot P^{h+3v} \equiv 0 \pmod{P^{h+3v+1}}. \tag{8}$$

Ora se $h = 0$ [e quindi $r \equiv s \equiv 0 \pmod 3$] la (8) ammette tutte le soluzioni di

$$\sigma^3 + A' \eta^3 - b_s \equiv 0 \pmod P, \qquad \text{ossia} \qquad \sigma^3 + a_r \cdot \eta^3 - b_s \equiv 0 \pmod P,$$

ove si ponga $\xi = P^v \sigma$, $y = P^v \eta$. Quest'ultima è certamente solubile per il Lemma A, con $0 < \eta < P$.

Da una tale soluzione σ, η si deduce una soluzione ξ, y della (8) e infine una soluzione x, y della (4), che soddisfa alle condizioni iniziali del Lemma C; grazie ad esso il Teorema vale dunque in questo caso.

Sia poi $h \neq 0$ [e quindi $r \equiv s \not\equiv 0 \pmod 3$].

Nella (8) dovrà essere $P \mid \xi$, e posto $\xi = P\sigma$ la (8) è equivalente a

$$P^{h'} \cdot \sigma^3 + A' y^3 - b_s \cdot P^{3v} \equiv 0 \pmod{P^{3v+1}}. \tag{9}$$

I primi due termini sono divisibili per potenze di P di esponente certamente diverso e pertanto deve essere $P^v \mid \sigma$, $P^v \mid y$; e poniamo $y = P^v \eta$.

La (9) è allora equivalente a

$$A'\eta^3 \equiv b_s \qquad \text{ossia} \qquad a_r\,\eta^3 \equiv b_s \pmod{P},$$

che è solubile se e soltanto se $a_r^{-1}\cdot b_s$ è residuo cubico di P, ed in caso affermativo si hanno soluzioni con $0 < \eta < P$.

Scelto σ arbitrario, purchè multiplo di P^v (per esempio posto $\sigma = 0$), si trova così una soluzione della (8), e di qui una della (4), che soddisfa alle condizioni del Lemma C; il Teorema A è così completamente dimostrato.