SULLA CONGRUENZA GENERALE DI 4° GRADO

SECONDO UN MODULO PRIMO.

Nota di **Gerolamo Cordone**, in Genova.[Adunanze del 12 e 26 maggio 1895.]

La teoria generale delle congruenze di 2°, 3° e 4° grado secondo un modulo primo fu iniziata da *Cauchy* nel vol. IV dei suoi *Exercices de Mathématiques*, ov'egli si limita però al caso in cui le congruenze in questione ammettono tante radici razionali, quante unità sonvi nel loro grado.

La discussione generale della congruenza di 3° grado fu compiuta da *Oltramare* (vol. 45 del *Journal von Crelle*), il quale non solo determinò le condizioni necessarie e sufficienti perchè la proposta ammetta una o più radici razionali, ma diè altresì l'espressione esplicita delle radici in funzione razionale dei coefficienti della congruenza e del suo modulo.

Per quanto riguarda la congruenza generale del 4° grado secondo un modulo primo, la questione, a nostra conoscenza, è ancora insoluta. È dunque di tale discussione che ci occuperemo in questo lavoro, dove, pure traendo partito dei risultati dell'*Oltramare* concernenti la congruenza generale di 3° grado, mostreremo come si possano in più punti semplificare e completare.

Ci limiteremo però a dare sotto forma razionale soltanto una o al più due radici della congruenza proposta, quand'anche essa ne ammetta un numero maggiore; e riguarderemo le espressioni della forma

$$\sqrt[m]{a}$$

(a razionale), come razionalmente note, semprechè la congruenza

$$x^m - a \equiv 0 \pmod{\mu}$$

sia risolubile.

1. Nella teoria delle congruenze irriducibili secondo un modulo primo, si dimostra che una congruenza qualunque di grado v , ammette v radici. Quindi la congruenza generale di 4° grado con modulo primo, ammetterà sempre quattro radici, razionali o no; e si potrà avere un'espressione analitica delle radici, ricorrendo agli stessi metodi coi quali si ottengono per radicali le radici della equazione di 4° grado.

Si tratterà poi di ricercare in quali casi le espressioni ottenute si riducono a numeri razionali.

Noi adotteremo il metodo dal prof. Giudice esposto nel vol. II della Rivista di Matematica (P e a n o).

2. Consideriamo la congruenza

$$(1) \quad y^4 + 4by^3 + 6cy^2 + 4dy + e \equiv 0 \pmod{\mu},$$

μ essendo un numero primo diverso da 2 e 3, e b, c, d, e numeri razionali qualunque.

Poniamo per brevità:

$$a) \quad H \equiv c - b^2$$

$$b) \quad I \equiv e - 4bd + 3c^2$$

$$c) \quad G \equiv d - 3bc^2 + 2b^3 \pmod{\mu}$$

$$d) \quad J \equiv \begin{vmatrix} 1 & b & c \\ b & c & d \\ c & d & e \end{vmatrix} \equiv HI - G^2 - 4H^3$$

$$e) \quad \Delta \equiv I^3 - 27J^2.$$

Se si pone :

$$(2) \quad x \equiv y + b \pmod{\mu},$$

la congruenza (1) si trasforma nella seguente :

$$A) \quad x^4 + 6Hx^2 + 4Gx + I - 3H^2 \equiv 0 \pmod{\mu}$$

che si può considerare come la forma generale della congruenza di 4° grado, H , G e $I - 3H^2 \equiv K \pmod{\mu}$ essendo numeri affatto arbitrarii.

Supponiamo che x sia della forma :

$$(3) \quad x \equiv t\sqrt[4]{\zeta} + \sqrt[4]{\zeta^2} + u\sqrt[4]{\zeta^3} \pmod{\mu},$$

t , ζ , u essendo quantità indeterminate. Indicando con α una radice primitiva della congruenza

$$\alpha^4 \equiv 1 \pmod{\mu}$$

si vede che il prodotto

$$P(x) \equiv \prod_{i=0}^{i=3} (x - \alpha^i t \sqrt[4]{\zeta} - \alpha^{2i} \sqrt[4]{\zeta^2} - \alpha^{3i} \sqrt[4]{\zeta^3}) \pmod{\mu}$$

si riduce a una funzione intera di 4° grado in x , i cui coefficienti sono razionali in t , u e ζ .

Confrontando le stesse potenze di x nella funzione $P(x)$ e nel 1° membro della proposta (A), si trovano tre equazioni di condizione nelle ζ , t e u e per eliminazione delle due ultime, si trae

$$B) \quad 4\zeta^3 + 12H\zeta^2 + (12H^2 - I)\zeta - G^2 \equiv 0 \pmod{\mu}$$

che si può chiamare la *risolvente* di 3° grado della congruenza (A) (*).

(*) La risolvente che si otterrebbe col metodo di Ferrari non differisce da quella del prof. Giudice che pel fattore 16 che in quella moltiplica tutte le radici.

Le radici $\zeta_1, \zeta_2, \zeta_3$ della (B) saranno date dalle formole:

$$\begin{aligned} \zeta_1 &\equiv -H + \frac{1}{2}(R_1 + R_2) \\ (4) \quad \zeta_2 &\equiv -H + \frac{1}{2}(fR_1 + f^2R_2) \pmod{\mu} \\ \zeta_3 &\equiv -H + \frac{1}{2}(f^2R_1 + fR_2) \end{aligned}$$

dove s'è posto per brevità:

$$\begin{aligned} (5) \quad R_1 &\equiv \sqrt[3]{-J + \sqrt{J^2 - \left(\frac{I}{3}\right)^3}} \quad R_2 \equiv \sqrt[3]{-J - \sqrt{J^2 - \left(\frac{I}{3}\right)^3}} \\ (6) \quad f &\equiv -\frac{1}{2} + \frac{\sqrt{-3}}{2} \quad f^2 \equiv -\frac{1}{2} - \frac{\sqrt{-3}}{2}. \end{aligned}$$

Indicando con x_1, x_2, x_3, x_4 le radici della proposta, si trova come nell'articolo citato del prof. Giudice:

$$(7) \quad \begin{cases} x_1 \equiv \sqrt{\bar{\zeta}_1} + \sqrt{\bar{\zeta}_2} + \sqrt{\bar{\zeta}_3} & x_3 \equiv -\sqrt{\bar{\zeta}_1} + \sqrt{\bar{\zeta}_2} - \sqrt{\bar{\zeta}_3} \\ x_2 \equiv \sqrt{\bar{\zeta}_1} - \sqrt{\bar{\zeta}_2} - \sqrt{\bar{\zeta}_3} & x_4 \equiv -\sqrt{\bar{\zeta}_1} - \sqrt{\bar{\zeta}_2} + \sqrt{\bar{\zeta}_3} \end{cases}$$

dove i segni dei radicali devono essere scelti in modo da verificare la relazione:

$$(8) \quad \sqrt{\bar{\zeta}_1} \sqrt{\bar{\zeta}_2} \sqrt{\bar{\zeta}_3} \equiv -\frac{G}{2}.$$

Si riconosce facilmente che se la funzione:

$$\Delta \equiv I^3 - 27J^2$$

è congrua a zero (mod μ), la cong. (A) ha delle radici uguali, e inversamente; perciò, adottando una denominazione propria della Teoria delle Equazioni, Δ può dirsi il *discriminante* della proposta.

3. Prima di studiare la congruenza (A) in tutta la sua genera-

lità, conviene considerare il caso particolare in cui si ha

$$G \equiv 0 \pmod{\mu}.$$

Allora la proposta si risolve come una congruenza di 2° grado, e si conclude facilmente il teorema seguente:

TEOREMA I.

a) Sia K un numero tale che sia

$$K^{\frac{\mu-1}{2}} \equiv +1 \pmod{\mu}.$$

La congruenza:

$$(9) \quad x^4 + 6Hx^2 + K \equiv 0 \pmod{\mu}$$

ammetterà quattro radici razionali o nessuna secondochè sia soddisfatta o no la condizione

$$(10) \quad (-3H + \sqrt{9H^2 - K})^{\frac{\mu-1}{2}} \equiv +1 \pmod{\mu}.$$

b) Se invece

$$K^{\frac{\mu-1}{2}} \equiv -1 \pmod{\mu},$$

la congruenza precedente ammetterà due radici razionali o nessuna, secondochè sarà o no verificata una delle due condizioni

$$(11) \quad (-3H + \sqrt{9H^2 - K})^{\frac{\mu-1}{2}} \equiv +1, \quad (-3H - \sqrt{9H^2 - K})^{\frac{\mu-1}{2}} \equiv -1.$$

c) Se infine

$$K \equiv 0 \pmod{\mu}$$

la cong. (9), che può scriversi

$$x^2(x^2 + 6H) \equiv 0 \pmod{\mu}$$

ammetterà (oltre alle due radici congrue a zero) due radici razionali o

nessuna secondochè si avrà :

$$(-6H)^{\frac{\mu-1}{2}} \equiv +1, \text{ oppure } (-6H)^{\frac{\mu-1}{2}} \equiv -1.$$

a) Se la condizione (10) è soddisfatta, non solo $\sqrt{9H^2 - K}$ è un numero razionale, ma $(-3H + \sqrt{9H^2 - K})$ è residuo quadratico secondo il modulo μ .

D'altronde, osservando che

$$(-3H + \sqrt{9H^2 - K})(-3H - \sqrt{9H^2 - K}) \equiv K$$

e quindi :

$$\begin{aligned} & (-3H + \sqrt{9H^2 - K})^{\frac{\mu-1}{2}} (-3H - \sqrt{9H^2 - K})^{\frac{\mu-1}{2}} \\ & \equiv (-3H - \sqrt{9H^2 - K})^{\frac{\mu-1}{2}} \equiv K^{\frac{\mu-1}{2}} \equiv +1 \end{aligned}$$

si vede che anche $(-3H - \sqrt{9H^2 - K})$ è residuo quadratico, epperò la proposta ammette quattro radici razionali, comprese nella formola

$$x \equiv \pm \sqrt{-3H \pm \sqrt{9H^2 - K}}.$$

Inversamente, se la (10) non è soddisfatta, $\sqrt{-3H + \sqrt{9H^2 - K}}$ e $\sqrt{-3H - \sqrt{9H^2 - K}}$ sono entrambe irrazionali; e la proposta non può ammettere alcuna radice razionale.

b) e c) Con un ragionamento analogo al precedente si riconosce l'esattezza della 2^a parte (b) del teorema; la 3^a parte, (c), è evidente, in forza della teoria delle congruenze binomie.

4. Le radici della cong. (9) possonsi esprimere razionalmente in funzione del modulo μ , dei coefficienti della congruenza e di una radice primitiva di μ .

È ciò che risulta dal teorema seguente, che è facile verificare.

TEOREMA II.—Sia $\mu = 2^m \mu_1 + 1$ (μ_1 impari) un numero primo,

a una radice primitiva pel numero μ , e N un numero tale che sia :

$$N^{\mu_1} \equiv a^{\frac{\mu-1}{2^{m-1}}} \pmod{\mu},$$

i essendo un termine determinato della serie 1, 2, ... 2^{m-1} .

Le radici della congruenza :

$$x^2 \equiv N \pmod{\mu}$$

saranno date dalla formola :

$$x \equiv \pm N^{\frac{\mu+1}{2}} a^{\frac{\mu-1}{2^m}} \pmod{\mu}.$$

5. Passando ora allo studio della congruenza :

$$(A) \quad x^4 + 6Hx^2 + 4Gx + K \equiv 0 \pmod{\mu}$$

considerata in tutta la sua generalità, converrà distinguere tre casi principali :

$$\text{I.} \quad -\frac{\Delta}{27} \equiv 0$$

$$\text{II.} \quad \left(-\frac{\Delta}{27}\right)^{\frac{\mu-1}{2}} \equiv +1 \pmod{\mu}$$

$$\text{III.} \quad \left(-\frac{\Delta}{27}\right)^{\frac{\mu-1}{2}} \equiv -1.$$

$$\text{I.} \quad -\frac{\Delta}{27} \equiv 0. \quad (C)$$

6. Applicando alla nostra congruenza (A) un ragionamento analogo a quello del Prof. Giudice circa la equazione del 4° grado a discriminante nullo, si conclude facilmente il seguente :

TEOREMA III. — Se I e J sono numeri tali che

$$-\frac{\Delta}{27} = J^2 - \left(\frac{I}{3}\right)^3 \equiv 0 \pmod{\mu}$$

la congruenza (A) ammetterà :

a) Per $J \equiv 0$, $H \not\equiv 0 \pmod{\mu}$ (*): Quattro radici razionali, di cui tre uguali fra loro, cioè:

$$x_1 \equiv 3\sqrt{-H} \equiv -\frac{6H^2}{G} \equiv \frac{3G}{2H}$$

$$x_2 \equiv x_3 \equiv x_4 \equiv -\sqrt{-H} \equiv \frac{2H^2}{G} \equiv -\frac{G}{2H}.$$

b) $J \not\equiv 0$, $J \equiv 8H^3 \not\equiv 0$:

$$\left\{ \begin{array}{l} (-3H)^{\frac{\mu-1}{2}} \equiv +1 \left\{ \begin{array}{l} \text{Due radici doppie razionali:} \\ x_1 \equiv x_2 \equiv +\sqrt{-3H}, \quad x_3 \equiv x_4 \equiv -\sqrt{-3H}. \end{array} \right. \\ (-3H)^{\frac{\mu-1}{2}} \equiv -1 \quad \text{Nessuna radice razionale.} \end{array} \right.$$

c) $J \not\equiv 0$, $J \not\equiv 8H^3$:

$$\left(-H + \frac{3J}{2I} \right)^{\frac{\mu-1}{2}} \equiv +1 \left\{ \begin{array}{l} \text{Una radice doppia razionale e due} \\ \text{semplici razionali:} \\ i) x_1 \equiv \sqrt{-H - \frac{3J}{I}} + 2\sqrt{-H + \frac{3J}{2I}} \\ \equiv -\frac{GI}{3J-2HI} + 2\sqrt{-H + \frac{3J}{2I}} \\ k) x_2 \equiv -\frac{GI}{3J-2HI} - 2\sqrt{-H + \frac{3J}{2I}} \\ x_3 \equiv x_4 \equiv -\sqrt{-H - \frac{3J}{I}} \equiv \frac{GI}{3J-2HI}. \end{array} \right.$$

$$\left(-H + \frac{3J}{2I} \right)^{\frac{\mu-1}{2}} \equiv -1 \left\{ \begin{array}{l} \text{Una radice doppia razionale:} \\ x_3 \equiv x_4 \equiv -\sqrt{-H - \frac{3J}{I}} \equiv \frac{GI}{3J-2HI} \end{array} \right.$$

(*) Adoperiamo in generale la notazione $a \not\equiv b \pmod{\mu}$ per indicare che a e b sono incongrui secondo il modulo μ .

OSSERVAZIONE. — Si potrebbe credere che, come lo s'è fatto nel caso a) pel radicale $\sqrt{-H}$, anche nel 3° caso, c), si possa esprimere direttamente $\sqrt{-H + \frac{3J}{2I}}$, e quindi x_1 e x_2 in funzione razionale dei coefficienti della proposta. Ma le formole che si otterrebbero in questo caso sono illusorie. Invero, se si pone per brevità:

$$\rho \equiv -\frac{GI}{3J-2HI} \equiv -\sqrt{\bar{\chi}_1}, \quad v \equiv 4\left(-H + \frac{3J}{2I}\right) \equiv 4\chi_2 \equiv 4\chi_3,$$

$x \equiv \rho \pm \sqrt{v}$ deve soddisfare identicamente alla congruenza (A), cioè si deve avere:

$$(12) \quad (\rho + \sqrt{v})^4 + 6H(\rho + \sqrt{v})^2 + 4G(\rho + \sqrt{v}) + K \equiv 0 \pmod{\mu}.$$

Donde segue

$$(13) \quad \sqrt{v} \equiv -\frac{v^2 + v(6\rho^2 + 6H) + \rho^2(6H + \rho^2) + 4G\rho + K}{4\rho v + 4\rho^3 + 12H\rho + 4G}.$$

Ed osservando che si ha, tenendo conto della (B):

$$4\rho^6 + 12H\rho^4 + (12H^2 - I)\rho^2 - G^2 \equiv 0$$

$$4\rho v + 4\rho^3 + 12H\rho + 4G \equiv 0$$

$$v^2 + v(6\rho^2 + 6H) + \rho^2(6H + \rho^2) + 4G\rho + K$$

$$\equiv \frac{1}{16\rho^2} [4\rho(6\rho^2 + 6H + v) - (4\rho^3 + 12H\rho + 4G)][4\rho v + 4\rho^3 + 12H\rho + 4G]$$

$$-\frac{1}{\rho^2} [4\rho^6 + 12H\rho^4 + (12H^2 - I)\rho^2 - G^2] \equiv 0 \pmod{\mu}$$

si vede che la frazione (13) si presenta sotto la forma indeterminata $\frac{0}{0}$.

$$\text{II.} \quad -\left(\frac{\Delta}{27}\right)^{\frac{\mu-1}{2}} \equiv +1. \quad (D)$$

7. Considereremo separatamente due casi, quello in cui il modulo μ è della forma $\mu = 6n - 1$, e quello in cui $\mu = 6n + 1$.

$$A) \quad \mu = 6n + 1.$$

Data la forma del numero μ , ed essendo per ipotesi $-\frac{\Delta}{27}$ residuo quadratico, la risolvente della proposta, cioè:

$$B) \quad 4\zeta^3 + 12H\zeta^2 + (12H^2 - I)\zeta - G^2 \equiv 0 \pmod{\mu}$$

ammette, com'è noto (*), una radice razionale ζ_1 , e due irrazionali ζ_2 e ζ_3 della forma:

$$(14) \quad \zeta_2 \equiv \varphi + \psi \sqrt{-3 \left(\frac{-\Delta}{27} \right)} \quad \zeta_3 \equiv \varphi - \psi \sqrt{-3 \left(\frac{-\Delta}{27} \right)}$$

φ e ψ essendo numeri razionali, e $\sqrt{-3 \left(\frac{-\Delta}{27} \right)} \equiv \sqrt{\Delta_1}$ essendo irrazionale per la forma del modulo μ , e per la (D).

Ciò posto, indichiamo con

$$(15) \quad x \equiv \varepsilon_1 \sqrt{\zeta_1} + \varepsilon_2 \sqrt{\zeta_2} + \varepsilon_3 \sqrt{\zeta_3} \pmod{\mu}$$

$$[\varepsilon_1^2 \equiv \varepsilon_2^2 \equiv \varepsilon_3^2 \equiv 1 \pmod{\mu}]$$

una qualunque delle radici della proposta, e facciamo successivamente le tre ipotesi seguenti:

$$a) \quad \zeta_1 \equiv 0$$

$$b) \quad \frac{\mu-1}{\zeta_1^2} \equiv -1$$

$$c) \quad \frac{\mu-1}{\zeta_1^2} \equiv +1$$

$$8. a) \quad \zeta_1 \equiv 0.$$

Se una delle radici della risolvente è nulla (mod. μ), si deve avere:

$$G \equiv 0 \pmod{\mu}$$

(*) Vedi *Oltremare* art. citato, Teor. II.

e quindi si ricade nel caso considerato al n° 3.

$$b) \quad \frac{\mu-1}{\bar{\chi}_1^2} \equiv -1.$$

Affinchè x sia razionale, bisogna che sia

$$x^\mu \equiv (\varepsilon_1 \sqrt{\bar{\chi}_1} + \varepsilon_2 \sqrt{\bar{\chi}_2} + \varepsilon_3 \sqrt{\bar{\chi}_3})^\mu \equiv \varepsilon_1 \sqrt{\bar{\chi}_1} + \varepsilon_2 \sqrt{\bar{\chi}_2} + \varepsilon_3 \sqrt{\bar{\chi}_3} \pmod{\mu}$$

cioè, osservando che

$$\begin{aligned} (\sqrt{\bar{\chi}_1})^\mu &\equiv -\sqrt{\bar{\chi}_1}, & (\sqrt{\bar{\chi}_2})^\mu &\equiv \sqrt{\bar{\chi}_2}, & (\sqrt{\bar{\chi}_3})^\mu &\equiv \sqrt{\bar{\chi}_2} \pmod{\mu}; \\ (16) \quad -2\varepsilon_1 \sqrt{\bar{\chi}_1} + (\varepsilon_2 - \varepsilon_3) \sqrt{\bar{\chi}_2} + (\varepsilon_3 - \varepsilon_2) \sqrt{\bar{\chi}_3} &\equiv 0. \end{aligned}$$

Se si potesse avere:

$$\varepsilon_2 \equiv \varepsilon_3$$

si avrebbe altresì:

$$\bar{\chi}_1 \equiv 0,$$

ciò che è contro l'ipotesi; dunque le radici x_1 e x_2 della proposta non possono essere razionali.

Le supposizioni:

$$\varepsilon_1 \equiv \varepsilon_3 \equiv -1, \quad \varepsilon_2 \equiv 1,$$

$$\varepsilon_1 \equiv \varepsilon_2 \equiv -1, \quad \varepsilon_3 \equiv 1,$$

corrispondenti rispettivamente alla terza e quarta radice della (A), conducono alle relazioni

$$(17) \quad \sqrt{\bar{\chi}_1} \equiv \sqrt{\bar{\chi}_2} - \sqrt{\bar{\chi}_3}, \quad \sqrt{\bar{\chi}_1} \equiv \sqrt{\bar{\chi}_3} - \sqrt{\bar{\chi}_2} \pmod{\mu}.$$

Dunque in questi due casi una delle radici della proposta è nulla (mod. μ). Si deve dunque avere:

$$K \equiv I - 3H^2 \equiv 0 \pmod{\mu}$$

e la proposta, soppressa la radice congrua a zero, si riduce alla congruenza di 3° grado :

$$(18) \quad x^3 + 6Hx + 4G \equiv 0 \pmod{\mu}.$$

Ora per ipotesi si ha :

$$-\frac{\Delta}{27} \equiv J^2 - \left(\frac{I}{3}\right)^3 \equiv J^2 - H^6 \equiv (J + H^3)(J - H^3) \equiv s^2 \pmod{\mu},$$

s essendo una quantità razionale.

E per la relazione d) n° 2 :

$$G^2 \equiv -J + H(I - 4H^2) \equiv -J - H^3$$

donde :

$$J + H^3 \equiv -G^2, \quad J - H^3 \equiv -G^2 - 2H^3,$$

$$G^2(G^2 + 2H^3) \equiv s^2, \quad G^2 + 2H^3 \equiv \left(\frac{s}{G}\right)^2 \pmod{\mu}.$$

Se si confronta la congruenza (18) colla seguente

$$(19) \quad x^3 + 3px + 2q \equiv 0 \pmod{\mu = 6n - 1}$$

di cui nel teorema II dell'Oltremare, si vede che :

$$(q^2 + p^3)^{\frac{\mu-1}{2}} \equiv [4G^2 + 2H^3]^{\frac{\mu-1}{2}} \equiv +1.$$

Dunque la (18) ammette una sola radice razionale, appartenente alla proposta (A).

Se si pone per brevità :

$$M \equiv \frac{1}{2} \{ [-2G + \sqrt{4G^2 + 8H^3}]^{2n} + [-2G - \sqrt{4G^2 + 8H^3}]^{2n} \}$$

le uniche radici razionali della proposta saranno

$$(20) \quad x \equiv 0, \quad x \equiv -\frac{2G}{H + M}.$$

9. Non sarà privo d'interesse il far vedere come si possa per-

venire in modo più semplice ai risultati consegnati nel teorema III dell'Oltremare, e concernenti la congruenza (19).

Posto :

$$(21) \quad S_1 \equiv \sqrt[3]{-q + \sqrt{q^2 + p^3}}, \quad S_2 \equiv \sqrt[3]{-q - \sqrt{q^2 + p^3}} \pmod{\mu}$$

$$(S_1 S_2 \equiv -p)$$

le radici della (19) saranno della forma :

$$(22) \quad x \equiv f^i S_1 + f^{2i} S_2 \quad (i = 0, 1, 2).$$

Ora l'espressione (22) non può essere razionale a meno che sia :

$$(f^i S_1 + f^{2i} S_2)^\mu \equiv f^{i\mu} S_1^\mu + f^{2i\mu} S_2^\mu \equiv f^i S_1 + f^{2i} S_2$$

cioè (essendo $f^{i\mu} \equiv f^{2i}$, $f^{2i\mu} \equiv f^i$, $S_1^\mu \equiv S_1$, $S_2^\mu \equiv S_2$):

$$f^i \equiv f^{2i}$$

ciò che esige che sia :

$$i \equiv 0.$$

L'unica radice razionale della (19) è dunque :

$$x \equiv S_1 + S_2.$$

D'altronde :

$$S_1^{6n} \equiv S_1^2 \equiv (-q + \sqrt{q^2 + p^3})^{2n} \pmod{\mu}$$

$$S_1 \equiv \varepsilon_1 (-q + \sqrt{q^2 + p^3})^n \quad (\varepsilon_1^2 \equiv 1)$$

da cui :

$$S_1^3 \equiv -q + \sqrt{q^2 + p^3} \equiv \varepsilon_1 (-q + \sqrt{q^2 + p^3})^{3n}$$

$$\varepsilon_1 \equiv (-q + \sqrt{q^2 + p^3})^{3n-1}.$$

Dunque :

$$x \equiv S_1 + S_2 \equiv (-q + \sqrt{q^2 + p^3})^{4n-1} - \frac{p}{(-q + \sqrt{q^2 + p^3})^{4n-1}}$$

$$\equiv (-q + \sqrt{q^2 + p^3})^{4n-1} + (-q - \sqrt{q^2 + p^3})^{4n-1}$$

ossia ponendo:

$$M' \equiv \frac{1}{2} \{ (-q + \sqrt{q^2 + p^3})^{4n-1} + (-q - \sqrt{q^2 + p^3})^{4n-1} \},$$

$$x \equiv 2 M' \pmod{\mu}.$$

Se si applicano queste formole alla congruenza (18) si trova:

$$(23) \quad x \equiv 2 M' \equiv [-2G + \sqrt{4G^2 + 8H^3}]^{4n-1} + [-2G - \sqrt{4G^2 + 8H^3}]^{4n-1}.$$

$$10. c) \quad \chi_1^{\frac{\mu-1}{2}} \equiv +1.$$

Se:

$$x \equiv \varepsilon_1 \sqrt{\chi_1} + \varepsilon_2 \sqrt{\chi_2} + \varepsilon_3 \sqrt{\chi_3}$$

è razionale, dovrà aversi:

$$(\varepsilon_1 \sqrt{\chi_1} + \varepsilon_2 \sqrt{\chi_2} + \varepsilon_3 \sqrt{\chi_3})^\mu$$

$$\equiv (\varepsilon_1 \sqrt{\chi_1} + \varepsilon_2 \sqrt{\chi_3} + \varepsilon_3 \sqrt{\chi_2}) \equiv \varepsilon_1 \sqrt{\chi_1} + \varepsilon_2 \sqrt{\chi_2} + \varepsilon_3 \sqrt{\chi_3}$$

cioè:

$$(\varepsilon_2 - \varepsilon_3) \sqrt{\chi_2} \equiv (\varepsilon_2 - \varepsilon_3) \sqrt{\chi_3},$$

donde, dovendo essere per ipotesi:

$$\sqrt{\chi_2} \neq \sqrt{\chi_3}$$

si ha:

$$\varepsilon_2 \equiv \varepsilon_3$$

Sicchè, se la proposta ammette delle radici razionali, soltanto le due prime, x_1 e x_2 , possono essere tali.

Ma se x è razionale, lo è pure $x - \sqrt{\chi_1}$, cioè:

$$x - \sqrt{\chi_1} \equiv \varepsilon_2 (\sqrt{\chi_2} + \sqrt{\chi_3}) \equiv \varepsilon_2 (\sqrt{\varphi + \psi \sqrt{\Delta_1}} + \sqrt{\varphi - \psi \sqrt{\Delta_1}}) \pmod{\mu}.$$

Ciò richiede che si possa porre :

$$(24) \quad \sqrt{\varphi + \psi \sqrt{\Delta_1}} \equiv \varphi_1 + \psi_1 \sqrt{\Delta_1},$$

φ_1 e ψ_1 indicando numeri razionali.

Reciprocamente, se la condizione (24) è soddisfatta, x_1 e x_2 sono razionali, e precisamente :

$$x_1 \equiv \sqrt{\Delta_1} + 2\varphi_1 \quad x_2 \equiv \sqrt{\Delta_1} - 2\varphi_1.$$

In virtù della teoria delle congruenze irriducibili, la condizione (24) equivale alla seguente :

$$(24') \quad \frac{\mu^2-1}{\chi_2^2} \equiv (\varphi + \psi t)^{\frac{\mu^2-1}{2}} \equiv 1 \pmod{\mu},$$

t essendo una radice della congruenza irriducibile

$$t^2 - \Delta_1 \equiv 0 \pmod{\mu}.$$

La condizione di possibilità (24') è soddisfatta di per sè. Infatti si ha :

$$\chi_2^{\mu+1} \equiv \chi_2 \chi_3 \pmod{\mu}.$$

Ed elevando i due membri alla potenza $\frac{\mu-1}{2} = 3n-1$:

$$\chi_2^{\frac{\mu^2-1}{2}} \equiv (\chi_2 \chi_3)^{\frac{\mu-1}{2}} \equiv \left(\frac{G^2}{4\chi_1}\right)^{\frac{\mu-1}{2}} \equiv \frac{\left(\frac{G}{2}\right)^{\mu-1}}{\chi_1^{\frac{\mu-1}{2}}} \equiv +1. \quad \text{C. V. D.}$$

Per esprimere le radici della proposta in funzione razionale dei coefficienti e del modulo, poniamo :

$$\left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{4n-1} \equiv R + S\sqrt{-\frac{\Delta}{27}} \pmod{\mu},$$

R e S indicando rispettivamente la parte indipendente da $\sqrt{-\frac{\Delta}{27}}$ e il

coefficiente di $\sqrt{-\frac{\Delta}{27}}$ nello sviluppo di $\left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{4n-1}$

secondo la formola del binomio.

Si avrà:

$$(25) \quad \begin{cases} R_1 \equiv \sqrt[3]{-J + \sqrt{-\frac{\Delta}{27}}} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{4n-1} \equiv R + S\sqrt{-\frac{\Delta}{27}} \\ R_2 \equiv \sqrt[3]{-J - \sqrt{-\frac{\Delta}{27}}} \equiv \left(-J - \sqrt{-\frac{\Delta}{27}}\right)^{4n-1} \equiv R - S\sqrt{-\frac{\Delta}{27}} \end{cases}$$

e quindi:

$$(26) \quad \begin{cases} \sqrt{\bar{\chi}_1} \equiv \sqrt{-H + R} \\ \sqrt{\bar{\chi}_2} \equiv \sqrt{-H - \frac{R}{2} + \frac{S}{2}\sqrt{\bar{\Delta}_1}} \equiv \varphi_1 + \psi_1 \sqrt{\bar{\Delta}_1} \\ \sqrt{\bar{\chi}_3} \equiv \sqrt{-H - \frac{R}{2} - \frac{S}{2}\sqrt{\bar{\Delta}_1}} \equiv \varphi_1 - \psi_1 \sqrt{\bar{\Delta}_1} \end{cases}$$

con:

$$\varphi \equiv -H - \frac{R}{2}, \quad \psi \equiv \frac{S}{2}.$$

Se si pone:

$$\chi_2^{3n-1} \equiv (\varphi + \psi \sqrt{\bar{\Delta}_1})^{3n-1} \equiv M + N \sqrt{\bar{\Delta}_1} \pmod{\mu}$$

(M e N essendo numeri razionali), si trova:

$$(27) \quad \begin{cases} (\sqrt{\bar{\chi}_2})^{6n-2} \equiv \chi_2^{3n-1} \equiv \frac{\sqrt{\bar{\chi}_3}}{\sqrt{\bar{\chi}_2}} \equiv \frac{\varphi_1 - \psi_1 \sqrt{\bar{\Delta}_1}}{\varphi_1 + \psi_1 \sqrt{\bar{\Delta}_1}} \equiv M + N \sqrt{\bar{\Delta}_1} \\ (\sqrt{\bar{\chi}_3})^{6n-2} \equiv \chi_3^{3n-1} \equiv \frac{\sqrt{\bar{\chi}_2}}{\sqrt{\bar{\chi}_3}} \equiv \frac{\varphi_1 + \psi_1 \sqrt{\bar{\Delta}_1}}{\varphi_1 - \psi_1 \sqrt{\bar{\Delta}_1}} \equiv M - N \sqrt{\bar{\Delta}_1} \end{cases}$$

da cui:

$$(28) \quad \begin{cases} \varphi_1 M + \psi_1 N \Delta_1 \equiv \varphi_1 \\ \varphi_1 N + \psi_1 M \equiv -\psi_1 \end{cases} \pmod{\mu}$$

all'una delle quali relazioni si può sostituire la seguente :

$$(29) \quad M^2 - N^2 \Delta_1 \equiv 1 \pmod{\mu}.$$

Dalle (26) si deduce poi :

$$(30) \quad \varphi \equiv \varphi_1^2 + \psi_1^2 \Delta_1$$

$$(31) \quad \psi \equiv 2 \varphi_1 \psi_1.$$

E dalle (28) e (31):

$$\psi_1 \equiv \pm \sqrt{-\frac{N\psi}{2(M+1)}},$$

per cui ψ_1 si può considerare come razionalmente noto in funzione dei coefficienti della proposta e del modulo.

Se si osserva che :

$$\sqrt{\bar{\chi}_2} \sqrt{\bar{\chi}_3} \equiv \varphi_1^2 - \psi_1^2 \Delta_1 \equiv -\frac{G}{2\sqrt{\bar{\chi}_1}},$$

si ottiene dalle (28), (29) e (31):

$$4\varphi_1^2 \equiv -\frac{G(M+1)}{\sqrt{\bar{\chi}_1}} \equiv \frac{\psi_1^2}{\psi_1^2} \equiv -\frac{2\psi(M+1)}{N} \equiv -\frac{S(M+1)}{N},$$

ossia :

$$\sqrt{\bar{\chi}_1} \equiv \frac{GN}{S}.$$

Dunque :

$$(32) \quad \begin{cases} x_1 \equiv \sqrt[3]{\bar{\chi}_1} + 2 \varphi_1 \equiv \frac{GN}{S} + \sqrt[3]{-\frac{S(M+1)}{N}} \\ x_2 \equiv \sqrt[3]{\bar{\chi}_1} - 2 \varphi_1 \equiv \frac{GN}{S} - \sqrt[3]{-\frac{S(M+1)}{N}} \end{cases} \pmod{\mu}. (*)$$

11. I risultati di cui ai numeri 9 e 10 si possono riassumere nel seguente teorema :

TEOREMA IV. — *Siano J e I numeri tali che :*

$$\left(-\frac{\Delta}{27}\right)^{\mu-1} \equiv +1 \pmod{\mu = 6n-1}$$

e posto :

$$R_1 \equiv \sqrt[3]{-J + \sqrt[3]{-\frac{\Delta}{27}}} \equiv \left(-J + \sqrt[3]{-\frac{\Delta}{27}}\right)^{4n-1} \equiv R + S \sqrt[3]{-\frac{\Delta}{27}} \pmod{\mu}$$

sia :

$$\chi_1 \equiv -H + R$$

l'unica radice razionale della cong. (B). Se :

a) $\chi_1^{\frac{\mu-1}{2}} \equiv -1$, la congruenza (A) ammetterà due radici razionali date dalle formole :

$$\begin{aligned} x_1 &\equiv 0, \quad x_2 \equiv [-G + \sqrt[4]{4G^2 + 8H^3}]^{4n-1} \\ &\quad + [-2G - \sqrt[4]{4G^2 + 8H^3}]^{4n-1} \pmod{\mu}. \end{aligned}$$

(*) Se si cercasse di eliminare da queste ultime formole il radicale $\sqrt[3]{-\frac{S(M+1)}{N}}$, esprimendo che x_1 deve soddisfare identicamente alla proposta (A), si perverrebbe, come per le formole i) e k) (n° 6), a delle espressioni indeterminate.

$$b) \quad \bar{\alpha}_1^{\frac{\mu-1}{2}} \equiv +1, \text{ posto}$$

$$\left[\left(-H - \frac{R}{2} \right) + \frac{S}{2} \sqrt{\frac{\Delta}{9}} \right]^{3^{n-1}} \equiv M + N \sqrt{\frac{\Delta}{9}} \quad (M \text{ e } N \text{ razionali})$$

ammetterà due radici razionali date da:

$$x_1 \equiv \frac{GN}{S} + \sqrt{-\frac{S(M+1)}{N}} \quad x_2 \equiv \frac{GN}{S} - \sqrt{-\frac{S(M+1)}{N}}.$$

c) $\bar{\alpha}_1 \equiv 0$, la cong. (A) ammetterà delle radici razionali nei casi indicati dal Teor. I.

$$12). B) \quad \mu = 6n + 1.$$

Anche qui converrà distinguere tre casi:

$$a) \quad R_1^{\frac{\mu-1}{3}} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}} \right)^{2n} \equiv 1,$$

$$b) \quad R_1^{\frac{\mu-1}{3}} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}} \right)^{2n} \equiv f,$$

$$c) \quad R_1^{\frac{\mu-1}{3}} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}} \right)^{2n} \equiv f^2.$$

$$13. a) \quad R_1^{\frac{\mu-1}{3}} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}} \right)^{2n} \equiv 1 \pmod{\mu}.$$

In quest'ipotesi la risolvente della congruenza proposta ammette tre radici razionali; vediamo quel che accada della proposta.

Osserviamo anzitutto che, ammetta o no delle radici razionali la (A), due al più delle radici $\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3$ della risolvente possono essere non residui quadratici secondo il modulo μ . Invero si ha:

$$(\bar{\alpha}_1 \bar{\alpha}_2 \bar{\alpha}_3)^{\frac{\mu-1}{2}} \equiv \left(\frac{G^2}{4} \right)^{\frac{\mu-1}{2}} \equiv +1.$$

Ma è anche facile riconoscere che se la proposta ammette delle radici razionali, tutte e tre le ζ sono residui quadratici. Invero, se si potesse avere ad es.:

$$\zeta_2^{\frac{\mu-1}{2}} \equiv \zeta_3^{\frac{\mu-1}{2}} \equiv -1, \quad \zeta_1^{\frac{\mu-1}{2}} \equiv +1$$

seguirebbe, supposto x razionale,

$$x^\mu \equiv \varepsilon_1 \sqrt[\mu]{\zeta_1} - \varepsilon_2 \sqrt[\mu]{\zeta_2} - \varepsilon_3 \sqrt[\mu]{\zeta_3} \equiv \varepsilon_1 \sqrt[\mu]{\zeta_1} + \varepsilon_2 \sqrt[\mu]{\zeta_2} + \varepsilon_3 \sqrt[\mu]{\zeta_3},$$

donde:

$$\zeta_2 \equiv \zeta_3,$$

ciò che non può essere, perchè $\left(-\frac{\Delta}{27}\right)^{\frac{\mu-1}{2}} \equiv +1$.

Dunque, affinchè la congruenza (A) ammetta delle radici razionali, bisogna che siano soddisfatte due delle condizioni:

$$(33) \quad \zeta_1^{\frac{\mu-1}{2}} \equiv \zeta_2^{\frac{\mu-1}{2}} \equiv \zeta_3^{\frac{\mu-1}{2}} \equiv 1 \pmod{\mu},$$

la terza essendo conseguenza delle altre due.

Reciprocamente, se le (33) sono verificate, la proposta ammette quattro radici razionali.

Poichè si sanno esprimere le ζ in funzione razionale dei dati, possiamo considerare come razionalmente note $\sqrt[\mu]{\zeta_1}$, $\sqrt[\mu]{\zeta_2}$, $\sqrt[\mu]{\zeta_3}$, e quindi anche le radici della proposta.

Tenendo conto di questi risultati e del teorema II, si può enunciare quanto segue:

TEOREMA V. — Sia il numero $\mu = 2^m \mu_1 + 1$ (μ_1 impari) della forma $\mu = 6n + 1$, e siano J e I numeri tali che:

$$\left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{2n} \equiv 1 \pmod{\mu}.$$

Sia inoltre α una radice primitiva pel numero μ .

La congruenza (A) ammetterà quattro radici razionali o nessuna

secondochè saranno o no soddisfatte le due condizioni:

$$(34) \quad \begin{cases} \zeta_1^{\frac{\mu-1}{2}} \equiv \left[-H + \frac{1}{2}(R_1 + R_2) \right]^{\frac{\mu-1}{2}} \equiv +1 \pmod{\mu} \\ \zeta_2^{\frac{\mu-1}{2}} \equiv \left[-H + \frac{1}{2}(fR_1 + f^2R_2) \right]^{\frac{\mu-1}{2}} \equiv +1 \pmod{\mu}. \end{cases}$$

Se, le condizioni (34) essendo verificate, si ha:

$$\zeta_1^{\mu_1} \equiv a^{\frac{\mu-1}{2^{m-1}}} \quad \zeta_2^{\mu_1} \equiv a^{\frac{k(\mu-1)}{2^{m-1}}} \pmod{\mu}$$

(i e k essendo due dei numeri $1, 2, \dots, 2^{m-1}$) una delle radici della proposta sarà data dalla formola:

$$x \equiv \frac{\left[-H + \frac{1}{2}(R_1 + R_2) \right]^{\frac{\mu_1+1}{2}}}{a^{\frac{\mu-1}{2^m}}} + \frac{\left[-H + \frac{1}{2}(fR_1 + f^2R_2) \right]^{\frac{\mu_1+1}{2}}}{a^{\frac{k(\mu-1)}{2^m}}} - \frac{G a^{\frac{(i+k)(\mu-1)}{2^m}}}{2 \left\{ \left[-H + \frac{1}{2}(R_1 + R_2) \right] \left[-H + \frac{1}{2}(fR_1 + f^2R_2) \right] \right\}^{\frac{\mu_1+1}{2}}}.$$

COROLLARIO. — Se il numero $\mu = 6n + 1$ è pure della forma $4m + 3$ e se si pone:

$$\left[-H + \frac{1}{2}R_1 + \frac{I}{6\left(-J + \sqrt{-\frac{\Delta}{27}}\right)} R_1^2 \right]^{m+1} \equiv M + NR_1 + PR_1^2 \pmod{\mu}$$

(M , N e P essendo i coefficienti di R_1^0 , R_1^1 , R_1^2 nello sviluppo di

$$\left[-H + \frac{1}{2}R_1 + \frac{I}{6\left(-J + \sqrt{-\frac{\Delta}{27}}\right)} R_1^2 \right]^{m+1} \text{ secondo la formola del}$$

trinomio), una delle radici della proposta sarà data dalla formola:

$$x \equiv 3M \pmod{\mu}.$$

$$14. \quad b) \quad R_1^{\frac{\mu-1}{3}} \equiv \left(-J + \sqrt[3]{-\frac{\Delta}{27}} \right)^{2n} \equiv f \pmod{\mu}.$$

La risolvente della proposta non ammette in questo caso alcuna radice razionale, mentre, come vedremo, la proposta (A) ammette sempre una radice razionale.

In virtù della *b)*

$$R_2^{\frac{\mu-1}{3}} \equiv \left(-J + \sqrt[3]{-\frac{\Delta}{27}} \right)^{2n} \equiv f^2$$

da cui :

$$(V\bar{\chi}_1)^\mu \equiv V\bar{\chi}_2, \quad (V\bar{\chi}_2)^\mu \equiv V\bar{\chi}_3, \quad (V\bar{\chi}_3)^\mu \equiv V\bar{\chi}_1,$$

dunque se x è razionale,

$$\begin{aligned} x^\mu &\equiv (\varepsilon_1 V\bar{\chi}_1 + \varepsilon_2 V\bar{\chi}_2 + \varepsilon_3 V\bar{\chi}_3)^\mu \\ &\equiv \varepsilon_1 V\bar{\chi}_2 + \varepsilon_2 V\bar{\chi}_3 + \varepsilon_3 V\bar{\chi}_1 \equiv \varepsilon_1 V\bar{\chi}_1 + \varepsilon_2 V\bar{\chi}_2 + \varepsilon_3 V\bar{\chi}_3 \end{aligned}$$

cioè :

$$(35) \quad (\varepsilon_1 - \varepsilon_3) V\bar{\chi}_1 + (\varepsilon_2 - \varepsilon_1) V\bar{\chi}_2 + (\varepsilon_3 - \varepsilon_2) V\bar{\chi}_3 \equiv 0.$$

La (35) prova che essendo per ipotesi tutte distinte le χ , se la proposta ammette delle radici razionali, una sola, la x_1 , può essere tale.

D'altra parte, perchè x_1 sia razionale, è necessario e sufficiente che si possa porre :

$$\begin{aligned} V\bar{\chi}_1 &\equiv \sqrt[3]{-H + \frac{1}{2} R_1 f^{i-1} + \frac{I}{6 \left(-J + \sqrt[3]{-\frac{\Delta}{27}} \right)} R_1^2 f^{2(i-1)}} \\ &\equiv M + N f^i R_1 + P f^{2i} R_1^2 \end{aligned}$$

(M, N, P essendo numeri razionali), od anche indicando con t una radice della congruenza irriducibile :

$$t^3 \equiv -J + \sqrt[3]{-\frac{\Delta}{27}} \pmod{\mu}$$

che si abbia :

$$(36) \left[-H + \frac{I}{2} t + \frac{I}{6 \left(-J + \sqrt{\frac{-\Delta}{27}} \right)} t^2 \right]^{\frac{\mu^3-1}{2}} \equiv 1 \pmod{\mu}.$$

Ora la condizione precedente è sempre verificata; infatti si ha (i essendo uno qualunque dei numeri 1, 2, 3):

$$\zeta_i^{\frac{(6n+1-i)(6n+1^2+6n+1+i)}{2}} \equiv \zeta_i^{3n(6n+1^2+6n+1+i)} \equiv \zeta_{i+2}^{3n} \cdot \zeta_{i+1}^{3n} \cdot \zeta_i^{3n} \equiv \left(\frac{G^2}{4} \right)^{3n} \equiv 1 \pmod{\mu}.$$

Dunque la proposta ammette effettivamente una radice razionale.

15. Per ottenere questa radice in funzione razionale dei coefficienti e del modulo, osserviamo che dalle congruenze

$$\zeta_i^{3n} V_{\zeta_i}^- \equiv V_{\zeta_{i+1}}^- \quad (i = 1, 2, 3)$$

$$V_{\zeta_1}^- V_{\zeta_2}^- V_{\zeta_3}^- \equiv -\frac{G}{2}$$

si deduce :

$$V_{\zeta_1}^- \equiv -\frac{G}{2 \zeta_2^{3n+1}} \equiv -\frac{2}{G} (\zeta_1 \zeta_2)^{3n+1} \equiv M + NfR_1 + Pf^2R_1^2$$

$$V_{\zeta_2}^- \equiv -\frac{G}{2 \zeta_3^{3n+1}} \equiv -\frac{2}{G} (\zeta_1 \zeta_2)^{3n+1} \equiv M + Nf^2R_1 + PfR_1^2$$

$$V_{\zeta_3}^- \equiv -\frac{G}{2 \zeta_1^{3n+1}} \equiv -\frac{2}{G} (\zeta_2 \zeta_3)^{3n+1} \equiv M + NR_1 + PR_1^2,$$

donde

$$x_1 \equiv 3M.$$

Possiamo quindi concludere il seguente teorema :

TEOREMA VI. — Se J e I sono numeri tali che si abbia :

$$\left(-J + \sqrt{\frac{-\Delta}{27}}\right)^{2n} \equiv f \equiv -\frac{1}{2} + \frac{\sqrt{-3}}{2} \pmod{\mu = 6n + 1}$$

la cong. (A) ammette una ed una sola radice razionale data dalla formola

$$x \equiv 3M,$$

M rappresentando la parte dello sviluppo di $-\frac{G}{2\chi_i^{n+1}}$ secondo le po-

tenze di $R_i \equiv \sqrt[3]{-J + \sqrt{-\frac{\Delta}{27}}}$, che non contiene R_i a fattore ».

$$16. c) R^{\frac{\mu-1}{3}} \equiv \left(-J + \sqrt{\frac{-\Delta}{27}}\right)^{2n} \equiv f^2 \equiv -\frac{1}{2} - \frac{\sqrt{-3}}{2} \pmod{\mu}.$$

Con un ragionamento perfettamente analogo, si conclude un teorema che non differisce affatto dal precedente.

$$\text{III. } \left(\frac{-\Delta}{27}\right)^{\frac{\mu-1}{2}} \equiv -1. \quad (E)$$

17. Anche qui conviene distinguere due casi principali; il caso in cui $\mu = 6n + 1$ e quello in cui $\mu = 6n - 1$.

A) $\mu = 6n + 1$.

Prima di affrontare lo studio della congruenza generale di 4° grado, mostreremo come debbano essere modificati i teoremi VII e VIII dell'Oltremare circa la congruenza di 3° grado :

$$(37) \quad x^3 + 3px + 2q \equiv 0 \pmod{\mu = 6n + 1},$$

per la quale si ha

$$(q^2 + p^3)^{\frac{\mu-1}{2}} \equiv -1 \pmod{\mu}.$$

Si riconosce dapprima, come all'art. 7, che posto

$$S_1 \equiv \sqrt[3]{-q + \sqrt{q^2 + p^3}}, \quad S_2 \equiv \sqrt[3]{-q - \sqrt{q^2 + p^3}}$$

la sola radice

$$x \equiv S_1 + S_2$$

della (37) può essere razionale.

Quindi, che se x è razionale, S_1 dovrà essere dalla forma

$$(38) \quad S_1 \equiv \alpha + \beta \sqrt{q^2 + p^3}$$

(α e β indicando quantità razionali).

In altri termini si deve avere

$$(39) \quad (-q + t)^{\frac{\mu^2 - 1}{3}} \equiv 1 \pmod{\mu},$$

essendo una radice della congruenza irriducibile

$$t^2 \equiv (q^2 + p^3) \pmod{\mu}$$

condizione che è verificata di per sè, perchè si ha :

$$(-q + t)^{(6n+1+1) \cdot 2n} \equiv (-q - t)^{2n} (-q + t)^{2n} \equiv (-p^3)^{2n} \equiv 1.$$

Dunque la (37) ammette sempre una radice razionale, la quale si trova facilmente essere :

$$(40) \quad x \equiv -\frac{1}{p} [(-q + \sqrt{q^2 + p^3})^{2n+1} + (-q - \sqrt{q^2 + p^3})^{2n+1}] \pmod{\mu}.$$

D'altronde con tutta facilità si verifica che questa espressione soddisfa effettivamente alla (37).

Secondo l'enunciato invece del teorema VII dell'Oltremare, la cong. (37) ammetterà o no una radice razionale, secondochè sarà

Rend. Circ. Matem., t. IX, parte 1^a.—Stampato il 25 giugno 1895. 30

o no soddisfatta la congruenza :

$$(41) \quad (2M - 1)^2(M + 1) \equiv -\frac{2q^2}{p^3} \pmod{\mu},$$

M indicando la parte razionale dell'espressione :

$$(-q + \sqrt{q^2 + p^3})^{2n}.$$

In base ai nostri risultati la condizione (41) dev'essere verificata identicamente; è ciò che si riconosce facilmente.

I teoremi VII e VIII dell'articolo più volte citato, la cui dimostrazione è abbastanza complicata, devono essere sostituiti dal seguente.

TEOREMA VII.—*Se μ è un numero primo della forma $\mu=6n+1$, e se p e q sono numeri tali che sia :*

$$(q^2 + p^3)^{\frac{\mu-1}{2}} \equiv -1 \pmod{\mu},$$

la congruenza :

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

ammetterà sempre una ed una sola radice razionale, data dalla formola :

$$x \equiv 2M',$$

dov'è :

$$M' \equiv -\frac{1}{2p} [(-q + \sqrt{q^2 + p^3})^{2n+1} + (-q - \sqrt{q^2 + p^3})^{2n+1}].$$

18. Passiamo ora a considerare la congruenza (A).

Siccome i ragionamenti a farsi non differiscono sostanzialmente da quelli più volte adoperati, ci contenteremo d'enunciare all'incirca i risultati.

TEOREMA VIII. — *Siano J e I numeri tali che sia :*

$$\left(-\frac{\Delta}{27}\right)^{\frac{\mu-1}{2}} \equiv \left[J^2 - \left(\frac{I}{3}\right)^3\right]^{\frac{\mu-1}{2}} \equiv -1 \pmod{\mu=6n+1}$$

e, posto:

$$\begin{aligned} R_1 &\equiv \sqrt[3]{-J + \sqrt{-\frac{\Delta}{27}}} \equiv \frac{3}{I} \left(-J + \sqrt{-\frac{\Delta}{27}} \right)^{2n+1} \\ &\equiv R + S \sqrt{-\frac{\Delta}{27}} \end{aligned}$$

sia

$$\chi_1 = -H + R$$

l'unica radice razionale della congruenza (B).

a) Se $\chi_1^{\frac{\mu-1}{2}} \equiv -1$, la congruenza (A) ammetterà due radici razionali date dalle formole:

$$\begin{aligned} x_1 &\equiv 0, \quad x_2 \equiv -\frac{1}{3H} [(-2G + \sqrt{4G^2 + 8H^3})^{2n+1} \\ &\quad + (-2G - \sqrt{4G^2 + 8H^3})^{2n+1}]. \end{aligned}$$

b) Se $\chi_1^{\frac{\mu-1}{2}} \equiv +1$, due radici razionali, date da

$$\begin{aligned} x_1 &\equiv \frac{GN}{S\sqrt{-3}} + \sqrt{-\frac{S\sqrt{-3}(M+1)}{N}} \\ x_2 &\equiv \frac{GN}{S\sqrt{-3}} - \sqrt{-\frac{S\sqrt{-3}(M+1)}{N}} \end{aligned}$$

dove M e N sono rispettivamente i coefficienti di $\left(\sqrt{-\frac{\Delta}{27}}\right)^0$ e $\left(\sqrt{-\frac{\Delta}{27}}\right)^1$ nello sviluppo secondo la formola del binomio dell'espressione:

$$\chi_2^{3n} \equiv \left[\left(-H - \frac{R}{2} \right) + \frac{\sqrt{-3}S}{2} \cdot \sqrt{-\frac{\Delta}{27}} \right]^{3n}.$$

c) Se $\chi_1 \equiv 0$, la congruenza (A) ammetterà delle radici razionali nei casi indicati dal teorema I.

19. B) $\mu = 6n - 1$.

Svolgeremo anzitutto alcune brevi considerazioni circa la congruenza :

$$(43) \quad x^3 + 3px + 2q \equiv 0 \pmod{\mu = 6n - 1}$$

p e q essendo tali che :

$$(44) \quad (q^2 + p^3)^{\frac{\mu-1}{2}} \equiv -1 \pmod{\mu}.$$

Si riconosce dapprima, come lo dimostra l'Oltremare (Teorema IX), che la (43) ammette tre radici razionali o nessuna. Se il primo caso ha luogo, l'espressione :

$$x \equiv \sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}} \equiv S_1 + S_2 \pmod{\mu}$$

deve ridursi a un numero razionale, e per ciò bisogna e basta che sia soddisfatta la congruenza

$$(45) \quad (-q + t)^{\frac{6n-1^2-1}{3}} \equiv 1 \pmod{\mu},$$

essendo t una radice della congruenza irriducibile

$$t^3 \equiv q^2 + p^3 \pmod{\mu}.$$

Ma si ha :

$$(-q + \sqrt{q^2 + p^3})^{6n} \equiv (-q + \sqrt{q^2 + p^3})(-q - \sqrt{q^2 + p^3}) \equiv -p^3,$$

donde :

$$(46) \quad (-q + \sqrt{q^2 + p^3})^{2n} \equiv -f^i p.$$

Similmente :

$$(-q - \sqrt{q^2 + p^3})^{2n} \equiv -f^{2i} p.$$

Dunque :

$$(-q + \sqrt{q^2 + p^3})^{2n(6n-2)} \equiv (-q - \sqrt{q^2 + p^3})^{2n} (-q + \sqrt{q^2 + p^3})^{2n} \equiv f^i;$$

e perciò la condizione (45) equivale alla seguente :

$$i = 0$$

od anche a :

$$(47) \quad (-q + \sqrt{q^2 + p^3})^{2n} \equiv -p.$$

Sicchè la congruenza (47) è condizione non solo necessaria, come aveva dimostrato l'Oltremare, ma anche sufficiente perchè la congruenza (43) ammetta delle radici razionali.

20. Da quanto procede, tenuto conto della teoria delle congruenze irriducibili, si deduce la proposizione seguente :

TEOREMA IX. — Sia $\mu = 6n - 1 = 6 \cdot 3^m n_1 - 1$ (n_1 primo con 3): sia inoltre $A \equiv a + b\sqrt{q^2 + p^3}$ (a e b razionali) una radice primitiva della congruenza :

$$x^{\mu-1} \equiv 1 \pmod{\mu}.$$

Se la cong. (43) ammette delle radici razionali, si avrà (essendo i uno dei numeri 1, 2, ... 3^m):

$$(-q + \sqrt{q^2 + p^3})^{2n_1} \equiv -\sqrt[3^m]{p} A^{i \frac{\mu-1}{3^m}},$$

$$(-q - \sqrt{q^2 + p^3})^{2n_1} \equiv -\sqrt[3^m]{p} A^{-i \frac{\mu-1}{3^m}}.$$

Se, inoltre, si pone :

$$(a + b\sqrt{q^2 + p^3})^{i \frac{\mu-1}{3^m+1}} \equiv P + Q\sqrt{q^2 + p^3}$$

con che :

$$(a + b\sqrt{q^2 + p^3})^{-i \frac{\mu-1}{3^m+1}} \equiv P - Q\sqrt{q^2 + p^3};$$

e inoltre :

$$(-q + \sqrt{q^2 + p^3})^{\frac{2n_1+1}{3}} \equiv M + N\sqrt{q^2 + p^3}$$

$$(-q - \sqrt{q^2 + p^3})^{\frac{2n_1-1}{3}} \equiv M_1 + N_1\sqrt{q^2 + p^3}$$

una delle radici della congruenza sarà data dalla formola:

$$(48) \quad x \equiv -\frac{2}{\sqrt[3^{m+1}]{p}}(MP - NQ) \pmod{\mu}$$

se:

$$n_1 = 3n_2 + 1;$$

oppure dalla formola:

$$(49) \quad x \equiv -2\sqrt[3^{m+1}]{p}(M_1P + N_1Q) \pmod{\mu}$$

se:

$$n_1 = 3n_2 + 2.$$

21. Passiamo ora alla congruenza di 4° grado (A); e distinguiamo tre casi; secondochè si ha:

$$a) \quad R_i^{\mu+1} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{2n} \equiv \frac{I}{3}$$

$$b) \quad R_i^{\mu+1} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{2n} \equiv f \frac{I}{3}$$

$$c) \quad R_i^{\mu+1} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{2n} \equiv f^2 \frac{I}{3}.$$

22. a). In questo caso la risolvente della proposta ammette tre radici razionali; e circa la congruenza (A) si conclude il seguente teorema, intieramente analogo al teorema V.

TEOREMA X. — Sia il numero $\mu = 2^m \mu_1 + 1$ (μ_1 impari) della forma $\mu = 6n + 1$, e siano J e I numeri tali che:

$$\left(-\frac{\Delta}{27}\right)^{\frac{\mu-1}{2}} \equiv -1, \quad \left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{2n} \equiv \frac{I}{3} \pmod{\mu}.$$

Sia inoltre α una radice primitiva pel numero μ .

La congruenza (A) ammetterà quattro radici razionali o nessuna secondoche saranno o no soddisfatte le due condizioni:

$$(50) \quad \begin{cases} \zeta_1^{\frac{\mu-1}{2}} \equiv \left[-H + \frac{1}{2}(R_1 + R_2) \right]^{\frac{\mu-1}{2}} \equiv +1 \pmod{\mu} \\ \zeta_2^{\frac{\mu-1}{2}} \equiv \left[-H + \frac{1}{2}(fR_1 + f^2R_2) \right]^{\frac{\mu-1}{2}} \equiv +1 \pmod{\mu}. \end{cases}$$

Se, le condizioni precedenti essendo verificate, si ha:

$$\zeta_1^{\mu_1} \equiv a^{\frac{\mu_1-1}{2^{m-1}}} \quad \zeta_2^{\mu_1} \equiv a^{\frac{k\mu_1-1}{2^{m-1}}}$$

(i e k essendo due dei numeri 1, 2, ..., 2^{m-1}) una delle radici della proposta sarà data dalla formola:

$$x \equiv \frac{\zeta_1^{\frac{\mu_1+1}{2}}}{a^{\frac{\mu_1-1}{2^m}}} + \frac{\zeta_2^{\frac{\mu_1+1}{2}}}{a^{\frac{k\mu_1-1}{2^m}}} - \frac{Ga^{(i+k)\frac{\mu_1-1}{2^m}}}{(\zeta_1\zeta_2)^{\frac{\mu_1+1}{2}}} \pmod{\mu}.$$

COROLLARIO. — Se il numero $\mu = 6n - 1$ è pure della forma $12m + 11$, e se si pone:

$$\begin{aligned} \zeta_1^{3(m+1)} &\equiv \left[-H + \frac{1}{2}R_1 + \frac{I}{6\left(-J + \sqrt{-\frac{\Delta}{27}}\right)} R_1^2 \right]^{3(m+1)} \\ &\equiv M + NR_1 + PR_1^2 \pmod{\mu} \end{aligned}$$

(M, N, P essendo rispettivamente i coefficienti di R^0 , R^1 , R^2 nello sviluppo di $\zeta_1^{3(m+1)}$ secondo la formola del trinomio), una delle radici della proposta sarà data dalla formola:

$$x \equiv 3M \pmod{\mu}.$$

$$23. \quad b) \quad \left(-J + \sqrt{-\frac{\Delta}{27}} \right)^{2n} \equiv f \frac{I}{3}$$

In questo caso si ha:

(51) $\zeta_1^\mu \equiv \zeta_3, \quad \zeta_2^\mu \equiv \zeta_1, \quad \zeta_3^\mu \equiv \zeta_2 \pmod{\mu}$
 e quindi si riconosce subito che la sola radice x_1 della congruenza (A) può essere razionale.

D'altronde una qualunque, ζ_i , delle radici della risolvente, è di questa forma:

$$(52) \quad \zeta_i \equiv -H + \frac{I}{2} f^{i-1} R_1 + \frac{I}{6 \left(-J + \sqrt{-\frac{\Delta}{27}} \right)} f^{2(i-1)} R_1^2 \\ \equiv \varphi + \psi R_1 + \tau R_1^2 \pmod{\mu},$$

φ , ψ e τ indicando funzioni razionali intere, a coefficienti razionali, di $\sqrt{-\frac{\Delta}{27}}$. Inoltre J e I sono tali (cong. b) che non si possono determinare, come nel caso precedente (a), due numeri razionali α e β , soddisfacenti alla relazione:

$$R_1 \equiv \sqrt[3]{-J + \sqrt{-\frac{\Delta}{27}}} \equiv \alpha + \beta \sqrt{-\frac{\Delta}{27}}.$$

Perchè dunque la proposta ammetta una radice razionale, è necessario e sufficiente che si possa porre:

$$(53) \quad \sqrt{\zeta_i} \equiv \sqrt{\varphi + \psi R_1 + \tau R_1^2} \equiv M + N f^i R_1 + P f^{2i} R_1^2 \pmod{\mu},$$

M , N , P essendo, come φ , ψ e τ , funzioni razionali intere, a coefficienti razionali, di $\sqrt{-\frac{\Delta}{27}}$.

Nella teoria delle congruenze binomie della forma:

$$(54) \quad X^m \equiv A(x) \pmod{F(x), \mu}$$

$[F(x)$ essendo una funzione intera di grado ν , irriducibile secondo il modulo primo μ , e m un divisore di $\mu^\nu - 1]$ si dimostra che la condizione necessaria e sufficiente per la risolubilità della (54) è

espressa dalla congruenza :

$$A^{\frac{\mu\nu-1}{m}} \equiv 1 \quad [\text{modd. } F(x), \mu].$$

Similmente, la congruenza a triplice modulo :

$$(55) \quad Y(x, X)^m \equiv A(x, X) \quad [\text{modd. } G(x, X), F(x), \mu]$$

[$F(x)$ essendo sempre una funzione di grado ν , irriducibile secondo μ ; $G(x, X)$ una funzione intera di grado λ in X , i cui coefficienti sono polinomii in x , di grado inferiore a ν , il primo di essi essendo uguale all'unità; e tale che non si possa porre :

$$G(x, X) \equiv G_1(x, X)f(x, X) \quad [\text{modd. } F(x), \mu]$$

il grado di $G_1(x, X)$ in X essendo inferiore a λ ; e infine m essendo un divisore di $\mu^{\lambda\nu} - 1$], è possibile o no secondochè sia o no verificata la condizione :

$$(56) \quad A(x, X)^{\frac{\mu^{\lambda\nu}-1}{m}} \equiv 1 \quad [\text{mod. } G(x, X), F(x), \mu].$$

In particolare, prendendo :

$$F(x) = x^3 + \frac{\Delta}{27}, \quad G(x, X) = X^3 - (-J + x),$$

$$A(x, X) = \tau(x)X^2 + \psi(x)X + \varphi(x)$$

$$\mu = 6n - 1,$$

con che :

$$\nu = 2, \quad \lambda = 3, \quad m = 2,$$

si vede che la congruenza :

$$Y^2 \equiv \tau(x)X^2 + \psi(x)X + \varphi(x) \quad \left[\text{modd. } X^3 - (J+x), x^2 + \frac{\Delta}{27}, \mu \right]$$

è possibile ed allora soltanto, che si abbia :

$$(57) [\tau(x)X^2 + \psi(x)X + \varphi(x)]^{\frac{\mu-1}{2}} \equiv 1 \left[\text{mod. } X^3 - (-J+x), x^2 + \frac{\Delta}{27}, \mu \right].$$

Conveniamo ora che la indeterminata x sia una radice della congruenza irriducibile :

$$x^2 + \frac{\Delta}{27} \equiv 0 \pmod{\mu},$$

che, inoltre, X sia una radice della *congruenza irriducibile* a doppio modulo :

$$X^3 - (-J+x) \equiv 0 \left[\text{mod. } \left(x^2 + \frac{\Delta}{27} \right), \mu \right].$$

Allora si vede che la (53) sarà possibile ed allora soltanto che si abbia :

$$(58) \left[-H + \frac{I}{2}R_1 + \frac{I}{6\left(-J + \sqrt{-\frac{\Delta}{27}}\right)}R_1^2 \right]^{\frac{6n-1}{2}} \equiv 1 \pmod{\mu}.$$

Questa relazione è verificata identicamente in forza delle (51): dunque la proposta ammette sempre una radice razionale.

È facile quindi concludere la seguente proposizione :

TEOREMA XI.—Se J e I sono numeri tali che si abbia :

$$\left[J^2 - \left(\frac{I}{3} \right)^3 \right]^{\frac{\mu-1}{2}} \equiv \left(-\frac{\Delta}{27} \right)^{\frac{\mu-1}{2}} \equiv -1 \pmod{\mu = 6n-1}$$

$$R_1^{\mu+1} \equiv \left(-J + \sqrt{-\frac{\Delta}{27}} \right)^{2n} \equiv f \frac{I}{3},$$

la congruenza (A) ammetterà una sola radice razionale data dalla formola :

$$x \equiv 3M,$$

M rappresentando la parte dello sviluppo di

$$-\frac{G}{2\lambda_1^{3n}} \equiv -\frac{2(\lambda_2\lambda_3)^{3n}}{G} \equiv -\frac{2}{G} \left[-H + \frac{1}{2}fR_1 + \frac{I}{6\left(-J + \sqrt{-\frac{\Delta}{27}}\right)} f^2 R_1^2 \right]^{3n} \\ \times \left[-H + \frac{1}{2}f^2 R_1 + \frac{I}{6\left(-J + \sqrt{-\frac{\Delta}{27}}\right)} f R_1^2 \right]^{3n}$$

secondo le potenze di R_1 , che non contiene R_1 a fattore.

$$24. c) \quad \left(-J + \sqrt{-\frac{\Delta}{27}}\right)^{2n} \equiv f^2 \frac{I}{3}.$$

I ragionamenti e le conclusioni in questo 3° caso, non differiscono affatto da quelle del caso precedente.

Genova, maggio 1895.

GEROLAMO CORDONE.